Red Hat Satellite 5.6 Referenzhandbuch

Eine Anleitung für die erweiterten Funktionen von Red Hat Satellite
Ausgabe 1

John Ha
Athene Chan
Lana Brindley
David O'Brien
Daniel Macpherson

Red Hat Satellite 5.6 Referenzhandbuch

Eine Anleitung für die erweiterten Funktionen von Red Hat Satellite
Ausgabe 1

John Ha
Red Hat Engineering Content Services

Lana Brindley
Red Hat Engineering Content Services

Daniel Macpherson
Red Hat Engineering Content Services

Athene Chan
Red Hat Engineering Content Services

David O'Brien
Red Hat Engineering Content Services

Rechtlicher Hinweis

Copyright © 2013 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Zusammenfassung

Willkommen beim Red Hat Satellite 5.6 Referenzhandbuch. Das Red Hat Satellite Referenzhandbuch führt Sie durch die erweiterten Funktionen des Satellite Servers.

Inhaltsverzeichnis

Vorwort **7**
1. Zielgruppe 7
2. Dokumentkonventionen 7
2.1. Typografische Konventionen 7
2.2. Konventionen für Seitenansprachen 8
2.3. Anmerkungen und Warnungen 9
3. Hilfe bekommen und Feedback geben 10
3.1. Brauchen Sie Hilfe? 10
3.2. Wir freuen uns auf Ihr Feedback! 10

Kapitel 1. Red Hat Satellite Information **11**
1.1. Befehlszeilentools zur Konfigurationsverwaltung 11
1.1.1. Red Hat Network Actions Control 11
1.1.1.1. Allgemeine Befehlszeilenoptionen 11
1.1.2. Red Hat Network Configuration Client 12
1.1.2.1. Konfigurationsdateien auflisten 12
1.1.2.2. Konfigurationsdateien abrufen 13
1.1.2.3. Konfigurations-Channels ansehen 13
1.1.2.4. Unterschiede zwischen Konfigurationsdateien ermitteln 13
1.1.2.5. Konfigurationsdateien verifizieren 14
1.1.3. Red Hat Network Configuration Manager 14
1.1.3.1. Konfigurations-Channel erstellen 15
1.1.3.2. Dateien zu einem Konfigurations-Channel hinzufügen 15
1.1.3.3. Unterschiede zwischen neuesten Konfigurationsdateien ermitteln 16
1.1.3.4. Unterschiede zwischen verschiedenen Versionen ermitteln 17
1.1.3.5. Alle Dateien eines Channels herunterladen 18
1.1.3.6. Inhalte einer Datei abrufen 18
1.1.3.7. Alle Dateien in einem Channel auflisten 18
1.1.3.8. Alle Konfigurations-Channels auflisten 19
1.1.3.9. Eine Datei von einem Channel entfernen 19
1.1.3.10. Einen Konfigurations-Channel löschen 19
1.1.3.11. Die Anzahl der Datei-Revisionen ermitteln 20
1.1.3.12. Eine Datei in einem Channel aktualisieren 20
1.1.3.13. Mehrere Dateien gleichzeitig hochladen 20
1.2. Monitoring 21
1.2.1. Voraussetzungen 21
1.2.2. Konfigurieren des Red Hat Network Monitoring Daemon (rhnmd) 22
1.2.2.1. Installation des Red Hat Network Monitoring-Daemons 23
1.2.2.2. Konfiguration von SSH 24
1.2.2.3. Installation des SSH-Schlüssels 24
1.2.3. Konfigurieren des mysql Paketes für Probes 25
1.2.4. Aktivieren Benachrichtigungen 25
1.2.4.1. Erstellen von Benachrichtigungsmethoden 25
1.2.4.2. Erhalten von Benachrichtigungen 26
1.2.4.3. Umleiten von Benachrichtigungen 26
1.2.4.4. Löschen von Benachrichtigungsmethoden 27
1.2.5. Über Probes 28
1.2.5.1. Verwalten von Probes 28
1.2.5.2. Festlegen von Grenzwerten 29
1.2.5.3. Überwachung des Satellite Servers 29
1.2.6. Monitoring 30
1.2.6.1. Probe-Status 30

1.2.6.1.1. Probe-Status ⇒ Kritisch 31
1.2.6.1.2. Probe-Status ⇒ Warnung 31
1.2.6.1.3. Probe-Status ⇒ Unbekannt 31
1.2.6.1.4. Probe-Status ⇒ Ausstehend 31
1.2.6.1.5. Probe-Status ⇒ OK 32
1.2.6.1.6. Probe-Status ⇒ Alle 32
1.2.6.1.7. Aktueller Status 32
1.2.6.2. Benachrichtigung 32
1.2.6.2.1. Benachrichtigung ⇒ Filter 33
1.2.6.2.1.1. Benachrichtigung ⇒ Benachrichtigungsfilter ⇒ Aktive Filter 33
1.2.6.2.1.2. Benachrichtigung ⇒ Benachrichtigungs-Filter ⇒ Abgelaufene Filter 34
1.2.6.3. Probe-Suites 34
1.2.6.4. Scout Config Push 36
1.2.6.5. Allgemeine Monitoring-Konfiguration 36
1.3. Mehrfache Satellites 37
1.3.1. Inter-Satellite-Synchronisation 37
1.3.1.1. Manuelle Konfiguration 37
1.3.1.2. Automatisierte Konfiguration 40
1.3.2. Organisationssynchronisation 41
1.3.3. Inter-Satellite Synchronisation Anwendungsfälle 42

Kapitel 2. Red Hat Satellite und Solaris-spezifische Information 45
2.1. UNIX Unterstützungs-Handbuch 45
2.1.1. Einführung 45
2.1.1.1. Unterstützte UNIX-Varianten 45
2.1.1.2. Voraussetzungen 45
2.1.1.3. Enthaltene Features 45
2.1.1.4. Unterschiede in der Funktionalität 46
2.1.1.5. Ausgeschlossene Features 46
2.1.2. Satellite Server Vorbereitung/Konfiguration 47
2.1.3. Vorbereitung des Unix-Client-Systems 48
2.1.3.1. Herunterladen und Installation zusätzlicher Pakete 49
2.1.3.1.1. Pakete von Drittanbietern installieren 49
2.1.3.1.2. Suchpfad der Bibliothek konfigurieren 50
2.1.3.1.3. Red Hat Network-Client-Pakete herunterladen 50
2.1.3.1.4. Installieren der Red Hat Netzwerk-Pakete 51
2.1.3.1.5. Red Hat Network-Pakete in PATH einbinden 51
2.1.3.2. Implementieren der Client SSL-Zertifikate 52
2.1.3.3. Konfiguration der Clients 52
2.1.4. Registrierung und Updates für Unix-Clients 53
2.1.4.1. Registrieren von Unix-Systemen 53
2.1.4.2. Beziehen von Updates 53
2.1.4.2.1. Hochladen der Pakete auf den Satellite 54
2.1.4.2.1.1. solaris2mpm 54
2.1.4.2.1.2. rhnpush mit .mpm-Dateien 55
2.1.4.2.2. Durch die Website aktualisieren 56
2.1.4.2.3. rhnsd 56
2.1.4.2.4. Von der Befehlszeile aus aktualisieren 56
2.1.5. Remote-Befehle 57
2.1.5.1. Befehle aktivieren 57
2.1.5.2. Befehle ausführen 58

Kapitel 3. Red Hat Satellite Proxy Information 59
3.1. Verwendung des Red Hat Network Package Manager und die Lieferung Lokaler Pakete mittels Red Hat Network Proxy 59
3.1.1. Erstellen eines Privaten Channels 61

3.1.2. Hochladen von Paketen 61

Kapitel 4. Verwaltung von benutzerdefinierten Paketen 63
4.1. Erstellen von Paketen für Red Hat Network 63
4.1.1. Vorteile von RPM 63
4.1.2. Red Hat Network RPM-Richtlinien 64
4.2. Digitale Signaturen für Red Hat Network Pakete 65
4.2.1. GnuPG-Schlüsselpaar generieren 65
4.2.2. Pakete signieren 67
4.3. Import benutzerdefinierte GPG-Schlüssel 68

Kapitel 5. Suche und Bereinigung von Fehlern 70
5.1. Plattenplatz 70
5.2. Installieren und Aktualisieren 70
5.3. Dienstleistungen 71
5.4. Verbindungsfähigkeit 72
5.5. Protokollierung und Berichterstattung 73
5.6. Fehler 77
5.7. Weboberfläche 82
5.8. Anaconda 83
5.9. Tracebacks 84
5.10. Registrierung 85
5.11. Kickstarts und Snippets 86
5.12. Monitoring 87
5.13. Mehrfach-Organisationen Satellites und Satellite Zertifikate 88
5.14. Proxy Installation und Konfiguration 89

Probes 96
A.1. Probe-Richtlinien 96
A.2. Apache 1.3.x und 2.0.x 97
A.2.1. Apache::Processes 97
A.2.2. Apache::Traffic 98
A.2.3. Apache::Uptime 99
A.3. BEA WebLogic 6.x und höher 99
A.3.1. BEA WebLogic::Execute Queue 100
A.3.2. BEA WebLogic::Heap Free 101
A.3.3. BEA WebLogic::JDBC Connection Pool 101
A.3.4. BEA WebLogic::Server State 102
A.3.5. BEA WebLogic::Servlet 102
A.4. Allgemein 103
A.4.1. General::Remote Program 103
A.4.2. General::Remote Program with Data 104
A.4.3. General::SNMP Check 104
A.4.4. General::TCP Check 105
A.4.5. General::UDP Check (General::UDP Check) 105
A.4.6. General::Uptime (SNMP) 106
A.5. Linux 106
A.5.1. Linux::CPU Usage 107
A.5.2. Linux::Disk IO Throughput 107
A.5.3. Linux::Disk Usage 108
A.5.4. Linux::Inodes 109
A.5.5. Linux::Interface Traffic 109
A.5.6. Linux::Load 110
A.5.7. Linux::Memory Usage 111
A.5.8. Linux::Process Counts by State 111
A.5.9. Linux::Process Count Total 112

A.5.10. Linux::Process Health 113
A.5.11. Linux::Process Running 114
A.5.12. Linux::Swap Usage 115
A.5.13. Linux::TCP Connections by State 115
A.5.14. Linux::Users 116
A.5.15. Linux::Virtual Memory 116
A.6. LogAgent 117
A.6.1. LogAgent::Log Pattern Match 117
A.6.2. LogAgent::Log Size 118
A.7. MySQL 3.23 - 3.33 119
A.7.1. MySQL::Database Accessibility 119
A.7.2. MySQL::Opened Tables 120
A.7.3. MySQL::Open Tables 120
A.7.4. MySQL::Query Rate 120
A.7.5. MySQL::Threads Running 121
A.8. Netzwerkdienste 121
A.8.1. Network Services::DNS Lookup 121
A.8.2. Network Services::FTP 122
A.8.3. Network Services::IMAP Mail 122
A.8.4. Network Services::Mail Transfer (SMTP) 123
A.8.5. Network Services::Ping 123
A.8.6. Network Services::POP Mail 124
A.8.7. Network Services::Remote Ping 124
A.8.8. Network Services::RPCService 125
A.8.9. Network Services::Secure Web Server (HTTPS) 126
A.8.10. Network Services::SSH 126
A.8.11. Network Services::Web Server (HTTP) 127
A.9. Oracle 8i, 9i, 10g und 11g 127
A.9.1. Oracle::Active Sessions 128
A.9.2. Oracle::Availability 128
A.9.3. Oracle::Blocking Sessions 129
A.9.4. Oracle::Buffer Cache 129
A.9.5. Oracle::Client Connectivity 130
A.9.6. Oracle::Data Dictionary Cache 130
A.9.7. Oracle::Disk Sort Ratio 131
A.9.8. Oracle::Idle Sessions 131
A.9.9. Oracle::Index Extents 132
A.9.10. Oracle::Library Cache 132
A.9.11. Oracle::Locks 133
A.9.12. Oracle::Redo Log 133
A.9.13. Oracle::Table Extents 134
A.9.14. Oracle::Tablespace Usage 135
A.9.15. Oracle::TNS Ping 135
A.10. Red Hat Satellite 136
A.10.1. Red Hat Satellite::Disk Space 136
A.10.2. Red Hat Satellite::Ausführungszeit 136
A.10.3. Red Hat Satellite::Schnittstellen Verkehr 137
A.10.4. Red Hat Satellite::Latenz 137
A.10.5. Red Hat Satellite::Auslastung 137
A.10.6. Red Hat Satellite::Probe Anzahl 138
A.10.7. Red Hat Satellite::Prozess-Anzahl 138
A.10.8. Red Hat Satellite::Prozesse 139
A.10.9. Red Hat Satellite::Prozess Gesundheit 139
A.10.10. Red Hat Satellite::Prozess Laufend 140
A.10.11. Red Hat Satellite::Swap 141

A.10.12. Red Hat Satellite::Users 141

Versionsgeschichte **142**

Vorwort

1. Zielgruppe

Die Zielgruppe dieses Handbuchs sind **Systemadministratoren**, die Updates für Systeme innerhalb eines internen Netzwerks verwalten müssen.

2. Dokumentkonventionen

Dieses Handbuch verwendet mehrere Konventionen, um bestimmte Wörter und Sätze hervorzuheben und Aufmerksamkeit auf bestimmte Informationen zu lenken.

In PDF- und Papierausgaben verwendet dieses Handbuch Schriftbilder des Liberation-Fonts-Sets. Das Liberation-Fonts-Set wird auch für HTML-Ausgaben verwendet, falls es auf Ihrem System installiert ist. Falls nicht, werden alternative, aber äquivalente Schriftbilder angezeigt. Beachten Sie: Red Hat Enterprise Linux 5 und die nachfolgende Versionen beinhalten das Liberation-Fonts-Set standardmäßig.

2.1. Typografische Konventionen

Es werden vier typografische Konventionen verwendet, um die Aufmerksamkeit auf bestimmte Wörter und Sätze zu lenken. Diese Konventionen und die Umstände, unter denen sie auftreten, sind folgende:

`Nichtproportional Fett`

Dies wird verwendet, um Systemeingaben hervorzuheben, einschließlich Shell-Befehle, Dateinamen und -pfade. Es wird ebenfalls zum Hervorheben von Tasten und Tastenkombinationen verwendet. Zum Beispiel:

> Um den Inhalt der Datei **`my_next_bestselling_novel`** in Ihrem aktuellen Arbeitsverzeichnis zu sehen, geben Sie den Befehl **`cat my_next_bestselling_novel`** in den Shell-Prompt ein und drücken Sie **`Enter`**, um den Befehl auszuführen.

Das oben aufgeführte Beispiel beinhaltet einen Dateinamen, einen Shell-Befehl und eine Taste. Alle werden nichtproportional fett dargestellt und alle können, dank des Kontextes, leicht unterschieden werden.

Tastenkombinationen unterscheiden sich von einzelnen Tasten durch das Pluszeichen, das die einzelnen Teile einer Tastenkombination miteinander verbindet. Zum Beispiel:

> Drücken Sie **`Enter`**, um den Befehl auszuführen.
>
> Drücken Sie **`Strg`**+**`Alt`**+**`F2`**, um zu einem virtuellen Terminal zu wechseln.

Das erste Beispiel hebt die zu drückende Taste hervor. Das zweite Beispiel hebt eine Tastenkombination hervor: eine Gruppe von drei Tasten, die gleichzeitig gedrückt werden müssen.

Falls Quellcode diskutiert wird, werden Klassennamen, Methoden, Funktionen, Variablennamen und Rückgabewerte, die innerhalb eines Abschnitts erwähnt werden, wie oben gezeigt **`nichtproportional fett`** dargestellt. Zum Beispiel:

> Zu dateiverwandten Klassen zählen **`filesystem`** für Dateisysteme, **`file`** für Dateien und **`dir`** für Verzeichnisse. Jede Klasse hat ihren eigenen Satz an Berechtigungen.

Proportional Fett

Dies kennzeichnet Wörter oder Sätze, die auf einem System vorkommen, einschließlich Applikationsnamen, Text in Dialogfeldern, beschriftete Schaltflächen, Bezeichnungen für Auswahlkästchen und Radio-Buttons, Überschriften von Menüs und Untermenüs. Zum Beispiel:

> Wählen Sie **System** → **Einstellungen** → **Maus** in der Hauptmenüleiste aus, um die **Mauseinstellungen** zu öffnen. Wählen Sie im Reiter **Tasten** auf das Auswahlkästchen **Mit links bediente Maus** und anschließend auf **Schließen**, um die primäre Maustaste von der linken auf die rechte Seite zu ändern (d.h., um die Maus auf Linkshänder anzupassen).
>
> Um ein Sonderzeichen in eine **gedit**-Datei einzufügen, wählen Sie **Anwendungen** → **Zubehör** → **Zeichentabelle** aus der Hauptmenüleiste. Wählen Sie als Nächstes **Suchen** → **Suchen** aus der Menüleiste der **Zeichentabelle**, geben Sie im Feld **Suchbegriff** den Namen des Zeichens ein und klicken Sie auf **Weitersuchen**. Das gesuchte Zeichen wird daraufhin in der **Zeichentabelle** hervorgehoben. Doppelklicken Sie auf dieses hervorgehobene Zeichen, um es in das Feld **Zu kopierender Text** zu übernehmen und klicken Sie anschließend auf die Schaltfläche **Kopieren**. Gehen Sie nun zurück in Ihr Dokument und wählen Sie **Bearbeiten** → **Einfügen** aus der **gedit**-Menüleiste.

Der oben aufgeführte Text enthält Applikationsnamen, systemweite Menünamen und -elemente, applikationsspezifische Menünamen sowie Schaltflächen und Text innerhalb einer grafischen Oberfläche. Alle werden proportional fett dargestellt und sind anhand des Kontextes unterscheidbar.

Nichtproportional Fett Kursiv oder ***Proportional Fett Kursiv***

Sowohl bei nichtproportional fett als auch bei proportional fett weist ein zusätzlicher Kursivdruck auf einen ersetzbaren oder variablen Text hin. Kursivdruck kennzeichnet Text, der nicht wörtlich eingeben wird, oder angezeigten Text, der sich abhängig von den gegebenen Umständen unterscheiden kann. Zum Beispiel:

> Um sich mit einer Remote-Maschine via SSH zu verbinden, geben Sie an einem Shell-Prompt **ssh *username*@*domain.name*** ein. Falls die Remote-Maschine **example.com** ist und Ihr Benutzername auf dieser Maschine John lautet, geben Sie also **ssh john@example.com** ein.
>
> Der Befehl **mount -o remount *file-system*** hängt das angegebene Dateisystem wieder ein. Um beispielsweise das **/home**-Dateisystem wieder einzuhängen, verwenden Sie den Befehl **mount -o remount /home**.
>
> Um die Version des derzeit installierten Pakets zu sehen, verwenden Sie den Befehl **rpm -q *package***. Die Ausgabe sieht wie folgt aus: ***package-version-release***.

Beachten Sie die kursiv dargestellten Begriffe oben — username, domain.name, file-system, package, version und release. Jedes Wort ist ein Platzhalter entweder für Text, den Sie für einen Befehl eingeben, oder für Text, der vom System angezeigt wird.

Neben der Standardbenutzung für die Darstellung des Titels eines Werks zeigt der Kursivdruck auch die erstmalige Verwendung eines neuen und wichtigen Begriffs an. Zum Beispiel:

> Publican ist ein *DocBook* Publishing-System.

2.2. Konventionen für Seitenansprachen

Ausgaben des Terminals und Auszüge aus dem Quellcode werden visuell vom umliegenden Text hervorgehoben durch sogenannte Seitenansprachen (auch Pull-Quotes genannt).

Eine an das Terminal gesendete Ausgabe wird in den Schrifttyp **nichtproportional Roman** gesetzt und wie folgt dargestellt:

```
books        Desktop   documentation  drafts  mss    photos   stuff  svn
books_tests  Desktop1  downloads      images  notes  scripts  svgs
```

Auszüge aus dem Quellcode werden ebenfalls in den Schrifttyp **nichtproportional Roman** gesetzt, doch wird zusätztlich noch die Syntax hervorgehoben:

```
static int kvm_vm_ioctl_deassign_device(struct kvm *kvm,
                  struct kvm_assigned_pci_dev *assigned_dev)
{
         int r = 0;
         struct kvm_assigned_dev_kernel *match;

         mutex_lock(&kvm->lock);

         match = kvm_find_assigned_dev(&kvm->arch.assigned_dev_head,
                                       assigned_dev->assigned_dev_id);
         if (!match) {
                 printk(KERN_INFO "%s: device hasn't been assigned before, "
                   "so cannot be deassigned\n", __func__);
                 r = -EINVAL;
                 goto out;
         }

         kvm_deassign_device(kvm, match);

         kvm_free_assigned_device(kvm, match);

out:
         mutex_unlock(&kvm->lock);
         return r;
}
```

2.3. Anmerkungen und Warnungen

Zu guter Letzt verwenden wir drei visuelle Stile, um die Aufmerksamkeit auf Informationen zu lenken, die andernfalls vielleicht übersehen werden könnten.

Anmerkung

Eine Anmerkung ist ein Tipp, ein abgekürztes Verfahren oder ein alternativer Ansatz für die vorliegende Aufgabe. Das Ignorieren von Anmerkungen sollte keine negativen Auswirkungen haben, aber Sie verpassen so vielleicht einen Trick, der Ihnen das Leben vereinfachen könnte.

Warnung

Eine Warnung sollte nicht ignoriert werden. Das Ignorieren von Warnungen führt mit hoher Wahrscheinlichkeit zu Datenverlust.

3. Hilfe bekommen und Feedback geben

3.1. Brauchen Sie Hilfe?

Falls Sie Schwierigkeiten mit einer der in diesem Handbuch beschriebenen Prozeduren haben, besuchen Sie das Red Hat Kundenportal unter http://access.redhat.com. Via Kundenportal können Sie:

- eine Knowledgebase bestehend aus Artikeln rund um technischen Support für Red Hat Produkte durchsuchen oder zu durchstöbern.
- einen Support-Case bei Red Hat Global Support Services (GSS) einreichen.
- auf weitere Produktdokumentationen zugreifen.

Red Hat unterhält außerdem eine Vielzahl von Mailing-Listen zur Diskussion über Red Hat Software und Technologie. Eine Übersicht der öffentlich verfügbaren Listen finden Sie unter https://www.redhat.com/mailman/listinfo. Klicken Sie auf den Namen einer Liste für weitere Einzelheiten zum Abonnieren dieser Liste oder um auf deren Archiv zuzugreifen.

3.2. Wir freuen uns auf Ihr Feedback!

Wenn Sie einen Fehler in diesem Handbuch finden oder eine Idee haben, wie dieses verbessert werden könnte, freuen wir uns über Ihr Feedback! Reichen Sie einen Fehlerbericht für die Komponente **Red Hat Network Satellite** in Bugzilla unter http://bugzilla.redhat.com/ ein.

Vergewissern Sie sich beim Einreichen eines Fehlerberichts, dass Sie die Kennung des Handbuchs mit angeben: *Docs Reference Guide*

Falls Sie uns einen Vorschlag zur Verbesserung der Dokumentation senden möchten, sollten Sie hierzu möglichst genaue Angaben machen. Wenn Sie einen Fehler gefunden haben, geben Sie bitte die Nummer des Abschnitts und einen Ausschnitt des Textes an, damit wir diesen leicht finden können.

Kapitel 1. Red Hat Satellite Information

Dieser Abschnitt behandelt verschiedene Themen über Red Hat Satellite erweiterte Konfiguration.

1.1. Befehlszeilentools zur Konfigurationsverwaltung

Zusätzlich zu den Optionen, die durch die Red Hat Satellite Website zur Verfügung stehen, gibt es zwei Befehlszeilentools zur Verwaltung von Konfigurations-Dateien: den **Red Hat Network Configuration Client** und den **Red Hat Network Configuration Manager**. Der **Red Hat Network Actions Control** ist ein zusätzliches, kostenloses Tool, welches dazu verwendet werden kann, Konfigurations-Verwaltung auf Client-Systemen ein- und auszuschalten. Wenn Sie diese Werkzeuge bis jetzt noch nicht installiert haben, können Sie diese innerhalb des **`Red Hat Network Tools`**-Sub-Channels für Ihr Betriebssystem finden.

Tip

Wann immer eine Konfigurationsdatei via der Website eingesetzt wird, wird ein Backup der vorherigen Datei inklusive des vollständigen Pfads im Verzeichnis **`/var/lib/rhncfg/backups/`** auf dem betroffenen System erstellt. Das Backup behält den Dateinamen, bekommt aber eine **`.rhn-cfg-backup`** Erweiterung hinzugefügt.

1.1.1. Red Hat Network Actions Control

Die **Red Hat Network Actions Control** (**`rhn-actions-control`**) Applikation wird dazu verwendet, das Konfigurationsmanagement eines Systems zu aktivieren, bzw. zu deaktivieren. Client-Systeme können standardmäßig nicht auf diese Art verwaltet werden. Mit diesem Werkzeug können System-Verwalter bestimmte Betriebsarten der zulässigen Aktionen aktivieren sowie auch deaktivieren, wie beispielsweise: eine Konfigurationsdatei auf dem System *implementieren*, eine Datei vom System *hochladen*, ein *diff* erstellen von dem, was aktuell auf dem System verwaltet wird und dem, was erhältlich ist, oder *externe Befehle* durchführen. Diese unterschiedlichen Betriebsarten werden aktiviert/deaktiviert, indem Dateien und Verzeichnisse in das Verzeichnis **`/etc/sysconfig/rhn/allowed-actions/`** platziert oder daraus entfernt werden. Aufgrund der Standardberechtigungen auf dem **`/etc/sysconfig/rhn/`** Verzeichnis muss Red Hat Network Actions Control von einem Benutzer mit Root-Zugriff ausgeführt werden.

1.1.1.1. Allgemeine Befehlszeilenoptionen

Es gibt eine **`man`** Seite wie für die meisten Befehlszeilentools. Entscheiden Sie einfach, welche durch Red Hat Network eingeplanten Aktionen für die Verwendung durch System-Administratoren freigegeben werden sollen. Diese Optionen schalten die unterschiedlichen Verfahren für geplante Aktionen ein:

Tabelle 1.1. `rhn-actions-control`-Optionen

Option	Beschreibung
--enable-deploy	Erlaubt rhncfg-client, Dateien zu implementieren
--enable-diff	Erlaubt rhncfg-client, ein Diff von Dateien zu erstellen
--enable-upload	Erlaubt rhncfg-client, Dateien hochzuladen
--enable-mtime-upload	Erlaubt rhncfg-client, mtime hochzuladen
--enable-all	Erlaubt rhncfg-client, alles zu tun
--enable-run	Aktiviert script.run
--disable-deploy	Deaktiviert das Implementieren
--disable-diff	Deaktiviert diff
--disable-upload	Deaktiviert das Hochladen
--disable-mtime-upload	Deaktiviert mtime Hochladen
--disable-all	Deaktiviert alle Optionen
--disable-run	Deaktiviert script.run
--report	Berichtet, ob die Modi aktiviert oder deaktiviert sind
-f, --force	Erzwingt das Verfahren, ohne zuvor nachzufragen
-h, --help	Zeigt den Hilfebildschirm und beendet

Sobald ein Modus gesetzt ist, ist ihr System nunmehr für die Konfigurationsverwaltung durch Red Hat Network bereit.**`rhn-actions-control --enable-all`** ist eine gebräuchliche Option.

1.1.2. Red Hat Network Configuration Client

Wie der Name schon sagt, muss der **Red Hat Network Configuration Client** (**`rhncfg-client`**) auf einem individuellen Client-System installiert werden und dort laufen. Sie können anhand dieses Tools feststellen, wie Red Hat Network Konfigurationsdateien auf einem bestimmten System implementiert.

Der **Red Hat Network Configuration Client** bietet diese grundlegenden Verfahren: list, get, channels, diff und verify.

1.1.2.1. Konfigurationsdateien auflisten

Um die Konfigurationsdateien für den Rechner aufzulisten und die Labels der Konfigurations-Channels, welche diese beinhalten, führen Sie folgenden Befehl aus:

```
rhncfg-client list
```

Die Ausgabe ähnelt folgender Liste:

```
Config Channel      File
config-channel-17   /etc/example-config.txt
config-channel-17   /var/spool/aalib.rpm
config-channel-14   /etc/rhn/rhn.conf
```

Dies sind die Konfigurationsdateien, die auf Ihr System zutreffen. Es kann jedoch sein, dass sich Duplikate der Dateien in den anderen Channels befinden. Führen Sie beispielsweise folgenden Befehl aus:

```
rhncfg-manager list config-channel-14
```

und betrachten Sie folgende Ausgabe:

```
Files in config channel 'config-channel-14' /etc/example-config.txt
/etc/rhn/rhn.conf
```

Sie wundern sich dann vielleicht, wohin die zweite Version von **/etc/example-config.txt** verschwunden ist. Der Rang der **/etc/example-config.txt** Datei in **config-channel-17** war höher als der Rang derselben Datei in **config-channel-14**. Daher wird die Version der Konfigurationsdatei in **config-channel-14** nicht auf diesem System implementiert, obwohl sich die Datei noch immer im Channel befindet. Der **rhncfg-client** Befehl listet die Datei nicht auf, da diese auf dem System keinen Einsatz findet.

1.1.2.2. Konfigurationsdateien abrufen

Um die relevanteste Konfigurationsdatei für den Rechner herunterzuladen, führen Sie folgenden Befehl aus:

```
rhncfg-client get /etc/example-config.txt
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
Deploying /etc/example-config.txt
```

Sehen Sie die Inhalte der Datei mit **less** oder einem anderen Anzeigeprogramm an. Beachten Sie bitte dabei, dass die Datei als die relevanteste Datei basierend auf der Rangordnung des Konfigurations-Channels ausgewählt ist. Dies wird mittels dem Tab **Konfiguration** der **System-Details** Seite durchgeführt.

1.1.2.3. Konfigurations-Channels ansehen

Um die Labels und Namen der Konfigurations-Channels des Systems anzusehen, führen Sie folgenden Befehl aus:

```
rhncfg-client channels
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
Config channels: Label Name ----- ---- config-channel-17 config chan 2 config-
channel-14 config chan 1
```

Die folgende Tabelle listet die für **rhncfg-client get** vorhandenen Optionen auf:

Tabelle 1.2. rhncfg-client get Optionen

Option	Beschreibung
--topdir=TOPDIR	Führt alle Dateioperationen relativ zu diesem String aus.
--exclude=EXCLUDE	Schließt eine Datei aus mit 'get' eingesetzt zu werden / Kann mehrfach verwendet werden.
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.2.4. Unterschiede zwischen Konfigurationsdateien ermitteln

Um die Unterschiede zwischen den Konfigurationsdateien, die auf dem System implementiert sind und

den im Red Hat Network gespeicherten Dateien zu ermitteln, führen Sie folgenden Befehl aus:

```
rhncfg-client diff
```

Die Ausgabe sollte ungefähr so aussehen:

```
[root@testsatellite root]# rhncfg-client diff
--- /etc/test
+++ /etc/test 2013-08-28 00:14:49.405152824 +1000
@@ -1 +1,2 @@
 This is the first line
+This is the second line added
```

Zusätzlich dazu können Sie die Option **--topdir** hinzufügen, um Konfigurationsdateien in Red Hat Network mit denjenigen zu vergleichen, die sich auf einem beliebigen und freien Platz auf dem Client-System befinden:

```
[root@ root]# rhncfg-client diff --topdir /home/test/blah/ /usr/bin/diff:
/home/test/blah/etc/example-config.txt: No such file or directory /usr/bin/diff:
/home/test/blah/var/spool/aalib.rpm: No such file or directory
```

1.1.2.5. Konfigurationsdateien verifizieren

Um rasch festzustellen, ob Client-Konfigurationsdateien sich von denjenigen im Red Hat Network unterscheiden, führen Sie folgenden Befehl aus:

```
rhncfg-client verify
```

Die Ausgabe sollte ungefähr so aussehen:

```
modified /etc/example-config.txt /var/spool/aalib.rpm
```

Die Datei **example-config.txt** wurde lokal modifiziert, **aalib.rpm** hingegen nicht.

Die folgende Tabelle listet alle für **rhncfg-client verify** vorhandenen Optionen auf:

Tabelle 1.3. rhncfg-client verify Optionen

Option	Beschreibung
-v, --verbose	Erhöht die Ausführlichkeit der Bildschirmausgabe. Hierbei werden Unterschiede bezüglich Modus, Eigentümer und Gruppen-Berechtigungen für die angegebene Konfigurationsdatei angezeigt.
-o, --only	Nur Dateien mit Unterschieden anzeigen
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3. Red Hat Network Configuration Manager

Im Gegensatz zum **Red Hat Network Configuration Client** ist der **Red Hat Network Configuration Manager;** (**rhncfg-manager**) dazu entworfen, das zentrale Red Hat Network Repository von Konfigurations-Dateien und -Channels zu pflegen und nicht diejenigen auf den Client-Systemen. Dieses Tool stellt eine Befehlszeilen-Alternative zu den Konfigurations-Verwaltungs Features innerhalb der Red Hat Network Website dar und ermöglicht ebenso das Erstellen eines Skripts für einige

oder auch alle damit in Verbindung stehenden Wartungsaufgaben.

Es ist für die Benutzung durch Konfigurations-Administratoren vorgesehen und erfordert einen Red Hat Network Benutzernamen samt Passwort mit der entsprechenden Berechtigung. Der Benutzername kann in **/etc/sysconfig/rhn/rhncfg-manager.conf** oder im Abschnitt [rhncfg-manager] von **~/.rhncfgrc** festgelegt werden.

Wenn der **Red Hat Network Configuration Manager** als Root läuft, versucht dieser, die benötigten Konfigurationswerte vom **Red Hat Update Agent** einzuholen. Wenn dieser nicht als Root ausgeführt wird, müssen Sie eventuell Konfigurationsänderungen innerhalb der **~/.rhncfgrc** Datei durchführen. Die Sitzungsdatei ist in **~/.rhncfg-manager-session** zwischengespeichert, um zu verhindern, dass für jeden Befehl neu angemeldet werden muss.

Der standardmäßige Zeitablauf für den **Red Hat Network Configuration Manager** ist 30 Minuten. Um dies abzuändern, fügen Sie die Option **server.session_lifetime** und einen neuen Wert zu der **/etc/rhn/rhn.conf** Datei auf dem Server hinzu, auf dem der Manager läuft, wie z.B.:

```
server.session_lifetime = 120
```

Der **Red Hat Network Configuration Manager** bietet diese grundlegenden Modi: add, create-channel, diff, diff-revisions, download-channel, get, list, list-channels, remove, remove-channel, revisions, update und upload-channel.

Jeder Modus bietet seine eigene Reihe von Optionen, welche Sie mit dem folgenden Befehl ansehen können:

```
rhncfg-manager mode --help
```

Ersetzen Sie ***mode*** mit dem Namen des Modus, der angesehen werden soll:

```
rhncfg-manager diff-revisions --help
```

Sie finden eine solche Liste von Optionen für den add-Modus unter Tabelle 1.4, „**rhncfg-manager add** Optionen“.

1.1.3.1. Konfigurations-Channel erstellen

Um einen Konfigurations-Channel für Ihre Organisation zu erstellen, führen Sie folgenden Befehl aus:

```
rhncfg-manager create-channel channel-label
```

Wenn Sie nach Ihrem Red Hat Satellite Benutzernamen und Passwort gefragt werden, geben Sie diese ein. Die Ausgabe sieht wie folgt aus:

```
Red Hat Network username: rhn-user
Password:
Creating config channel channel-label Config channel channel-label created
```

Sobald Sie einen Konfigurations-Channel erstellt haben, stehen Ihnen die verbleibenden, oben aufgelisteten Modi zur Verfügung, um diesen Channel zu füllen und zu pflegen.

1.1.3.2. Dateien zu einem Konfigurations-Channel hinzufügen

Um eine Datei zu einem Konfigurations-Channel hinzuzufügen, geben Sie das Channel-Label sowie die lokale Datei zum Hochladen an, wie z.B.:

```
rhncfg-manager add --channel=channel-label /path/to/file
```

Zusätzlich zum erforderlichen Channel-Label und Pfad für die Datei können Sie die verfügbaren Optionen zur Modifikation der Datei benutzen. Beispielsweise können Sie den Pfad und den Dateinamen abändern, indem Sie die **--dest-file** Option zum Befehl hinzufügen:

```
rhncfg-manager add --channel=channel-label --dest-
file=/new/path/to/file.txt/path/to/file
```

Die Ausgabe sollte ungefähr so aussehen:

```
Pushing to channel example-channel
Local file >/path/to/file -> remote file /new/path/to/file.txt
```

Die folgende Tabelle listet alle für **rhncfg-manager add** verfügbaren Optionen auf:

Tabelle 1.4. rhncfg-manager add Optionen

Option	Beschreibung
-c CHANNEL --channel=CHANNEL	Lädt Dateien in diesen Konfigurations-Channel hoch
-d DEST_FILE --dest-file=DEST_FILE	Lädt die Datei als diesen Pfad hoch
--delim-start=DELIM_START	Starte Delimiter für variable Interpolation
--delim-end=DELIM_END	Beende Delimiter für varibale Interpolation
-i, --ignore-missing	Fehlende lokalen Dateien ignorieren
--selinux-context=SELINUX_CONTEXT	Überschreiben des SELinux-Kontext
-h, --help	Zeigt den Hilfebildschirm und beendet

Anmerkung

Standardmäßig beträgt die maximale Dateigröße für Konfigurationsdateien 128 KB. Falls Sie diesen Wert ändern müssen, suchen Sie die folgende Zeile (oder fügen diese hinzu) in der Datei **/etc/rhn/rhn.conf**:

```
web.maximum_config_file_size=128
```

Weiters suchen Sie die folgende Zeile (oder fügen diese hinzu) in der Datei **/etc/rhn/rhn.conf**:

```
maximum_config_file_size=128
```

Ändern Sie den Wert von 128 auf den gewünschten Wert in Bytes.

1.1.3.3. Unterschiede zwischen neuesten Konfigurationsdateien ermitteln

Um Unterschiede zwischen den Konfigurationsdateien auf der Festplatte und den neuesten Revisionen in einem Channel zu ermitteln, führen Sie den folgenden Befehl aus:

```
rhncfg-manager diff --channel=channel-label --dest-file=/path/to/file.txt \
/local/path/to/file
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
--- /tmp/dest_path/example-config.txt config_channel: example-channel revision: 1
+++ /home/test/blah/hello_world.txt 2003-12-14 19:08:59.000000000 -0500
@@ -1 +1 @@
-foo
+hello, world
```

Die folgende Tabelle listet alle für **`rhncfg-manager diff`** verfügbaren Optionen auf:

Tabelle 1.5. `rhncfg-manager diff` Optionen

Option	Beschreibung
-c CHANNEL, --channel=CHANNEL	Ruft Datei(en) von diesem Konfigurations-Channel ab
-r REVISION, --revision=REVISION	Verwende diese Revision
-d DEST_FILE, --dest-file=DEST_FILE	Lädt die Datei als diesen Pfad hoch
-t TOPDIR, --topdir=TOPDIR	Macht alle Dateien relativ zu diesem String
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.4. Unterschiede zwischen verschiedenen Versionen ermitteln

Um verschiedene Versionen einer Datei über Channels und Revisionen hinweg zu vergleichen, benutzen Sie die **`-r`** Flagge, um festzulegen, welche Revision der Datei verglichen werden soll und die **`-n`** Flagge, um die beiden Channels zu bestimmen, die überprüft werden sollen. Siehe Abschnitt 1.1.3.11, „Die Anzahl der Datei-Revisionen ermitteln“ für diesbezügliche Instruktionen. Geben Sie hier nur einen Dateinamen an, da Sie die Datei mit einer anderen Version von sich selbst vergleichen, wie beispielsweise:

```
rhncfg-manager diff-revisions -n=channel-label1 -r=1 -n=channel-label2 -r=1
/path/to/file.txt
```

Die Ausgabe sollte ungefähr so aussehen:

```
--- /tmp/dest_path/example-config.txt 2004-01-13 14:36:41 \ config channel:
example-channel2 revision: 1
--- /tmp/dest_path/example-config.txt 2004-01-13 14:42:42 \ config channel:
example-channel3 revision: 1
@@ -1 +1,20 @@
-foo
+blah
+-----BEGIN PGP SIGNATURE-----
+Version: GnuPG v1.0.6 (GNU/Linux)
+Comment: For info see http://www.gnupg.org
+
+iD8DBQA9ZY6vse4XmfJPGwgRAsHcAJ9ud9dabUcdscdcqB8AZP7e0Fua0NmKsdhQCeOWHX
+VsDTfen2NWdwwPaTM+S+Cow=
+=Ltp2
+-----END PGP SIGNATURE-----
```

Die folgende Tabelle listet die für **`rhncfg-manager diff-revisions`** verfügbaren Optionen auf:

Tabelle 1.6. `rhncfg-manager diff-revisions` Optionen

Option	Beschreibung
-c CHANNEL, --channel=CHANNEL	Verwende diesen Konfigurations-Channel
-r REVISION, --revision=REVISION	Verwende diese Revision
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.5. Alle Dateien eines Channels herunterladen

Um sämtliche Dateien in einem Channel auf Disk herunterzuladen, erstellen Sie ein Verzeichnis und führen Sie den folgenden Befehl aus:

```
rhncfg-manager download-channel channel-label --topdir .
```

Die Ausgabe sollte ungefähr so aussehen:

```
Copying /tmp/dest_path/example-config.txt -> \ blah2/tmp/dest_path/example-
config.txt
```

Die folgende Tabelle listet die für **`rhncfg-manager download-channel`** verfügbaren Optionen auf:

Tabelle 1.7. `rhncfg-manager download-channel` Optionen

Option	Beschreibung
-t TOPDIR, --topdir=TOPDIR	Verzeichnis, zu dem alle Dateipfade relativ sind. Diese Option muss angegeben sein.
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.6. Inhalte einer Datei abrufen

Um die Inhalte einer bestimmten Datei auf stdout (Standardausgabe) umzulenken, führen Sie den folgenden Befehl aus:

```
rhncfg-manager get --channel=channel-label \ /tmp/dest_path/example-config.txt
```

Sie sollten die Inhalte der Datei als Ausgabe sehen.

1.1.3.7. Alle Dateien in einem Channel auflisten

Um alle Dateien in einem Channel aufzulisten, führen Sie den folgenden Befehl aus:

```
rhncfg-manager list channel-label
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
Files in config channel `example-channel3': /tmp/dest_path/example-config.txt
```

Die folgende Tabelle listet die für **`rhncfg-manager get`** verfügbaren Optionen auf:

Tabelle 1.8. `rhncfg-manager get` Optionen

Option	Beschreibung
-c CHANNEL, --channel=CHANNEL	Ruft Datei(en) von diesem Konfigurations-Channel ab
-t TOPDIR, --topdir=TOPDIR	Macht alle Dateien relativ zu diesem String
-r REVISION, --revision=REVISION	Ruft diese Datei-Revision ab
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.8. Alle Konfigurations-Channels auflisten

Um alle Konfigurations-Channels Ihrer Organisation aufzulisten, führen Sie folgenden Befehl aus:

```
rhncfg-manager list-channels
```

Die Ausgabe sollte ungefähr so aussehen:

```
Available config channels: example-channel example-channel2 example-channel3
config-channel-14 config-channel-17
```

Beachten Sie, dass dies keine **`local_override`** oder **`server_import`**-Channels auflistet.

1.1.3.9. Eine Datei von einem Channel entfernen

Um eine Datei von einem Channel zu entfernen, führen Sie folgenden Befehl aus:

```
rhncfg-manager remove --channel=channel-label /tmp/dest_path/example-config.txt
```

Wenn Sie nach Ihrem Red Hat Network Benutzernamen und Passwort gefragt werden, geben Sie diese ein. Sie sollten eine Ausgabe ähnlich der folgenden erhalten:

```
Red Hat Network username: rhn-user Password: Removing from config channel example-
channel3 /tmp/dest_path/example-config.txt removed
```

Die folgende Tabelle listet die für **`rhncfg-manager remove`** verfügbaren Optionen auf:

Tabelle 1.9. `rhncfg-manager remove` Optionen

Option	Beschreibung
-c CHANNEL, --channel=CHANNEL	Entfernt Dateien von diesem Konfigurations-Channel
-t TOPDIR, --topdir=TOPDIR	Macht alle Dateien relativ zu diesem String
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.10. Einen Konfigurations-Channel löschen

Um einen Konfigurations-Channel in Ihrer Organisation zu löschen, führen Sie folgenden Befehl aus:

```
rhncfg-manager remove-channel channel-label
```

Die Ausgabe sollte ungefähr so aussehen:

```
Removing config channel example-channel Config channel example-channel removed
```

1.1.3.11. Die Anzahl der Datei-Revisionen ermitteln

Um herauszufinden, wie viele Revisionen (Revisionen gehen von 1 bis N, wobei N eine Ganzzahl größer als 0 ist) einer Datei oder von einem Pfad sich in einem Channel befinden, führen Sie den folgenden Befehl aus:

```
rhncfg-manager revisions channel-label /tmp/dest_path/example-config.txt
```

Die Ausgabe sollte ungefähr so aussehen:

```
Analyzing files in config channel example-channel \ /tmp/dest_path/example-
config.txt: 1
```

1.1.3.12. Eine Datei in einem Channel aktualisieren

Um eine neue Revision einer Datei in einem Channel zu erzeugen (oder um die erste Revision hinzuzufügen, wenn zuvor noch keine Revision für den jeweiligen Pfad existiert hat), führen Sie folgenden Befehl aus:

```
rhncfg-manager update \ --channel=channel-label --dest-file=/path/to/file.txt
/local/path/to/file
```

Die Ausgabe sollte ungefähr so aussehen:

```
Pushing to channel example-channel: Local file example-
channel/tmp/dest_path/example-config.txt -> \ remote file /tmp/dest_path/example-
config.txt
```

Die folgende Tabelle listet die für **`rhncfg-manager update`** verfügbaren Optionen auf:

Tabelle 1.10. `rhncfg-manager update` Optionen

Option	Beschreibung
-c CHANNEL, --channel=CHANNEL	Lädt Dateien in diesen Konfigurations-Channel hoch
-d DEST_FILE, --dest-file=DEST_FILE	Lädt die Datei als diesen Pfad hoch
-t TOPDIR, --topdir=TOPDIR	Macht alle Dateien relativ zu diesem String
--delim-start=DELIM_START	Starte Delimiter für variable Interpolation
--delim-end=DELIM_END	Beende Delimiter für varibale Interpolation
-h, --help	Zeigt den Hilfebildschirm und beendet

1.1.3.13. Mehrere Dateien gleichzeitig hochladen

Um mehrere Dateien von einer lokalen Disk auf einen Konfigurations-Channel hochzuladen, führen Sie den folgenden Befehl aus:

```
rhncfg-manager upload-channel --topdir=topdir channel-label
```

Die Ausgabe sollte ungefähr so aussehen:

```
Using config channel example-channel4 Uploading /tmp/ola_world.txt from
blah4/tmp/ola_world.txt
```

Die folgende Tabelle listet die für **`rhncfg-manager upload-channel`** verfügbaren Optionen auf:

Tabelle 1.11. `rhncfg-manager upload-channel` Optionen

Option	Beschreibung
-t TOPDIR, --topdir=TOPDIR	Verzeichnis, zu dem alle Dateipfade relativ sind
-c CHANNEL, --channel=CHANNEL	Liste von Channels, in welche die Konfigurationsinformationen hochgeladen werden. Channels werden durch ',' voneinander getrennt. Beispiel: --channel=foo,bar,baz
-h, --help	Zeigt den Hilfebildschirm und beendet

1.2. Monitoring

Die Red Hat Network Monitoring-Berechtigung ermöglicht es Ihnen, eine Reihe von Aktionen auszuführen, die dabei helfen sollen, Ihr System einwandfrei und effizient zu betreiben. Mithilfe des Monitorings können Sie Systemressourcen, Netzwerkdienste, Datenbanken, Standardapplikationen und benutzerdefinierte Applikationen genauestens überwachen.

Monitoring bietet sowohl Echtzeitinformationen als auch rückblickende Informationen zu Status-Änderungen und spezifischen Metriken. Es bietet Meldungen von Systemausfällen und Leistungseinbußen bevor sie kritisch werden sollten. Es bietet auch Informationen, welche die Kapazitätsplanung und Ereigniskorrelation unterstützen. So würde beispielsweise eine Probe (Tester), welche die CPU-Auslastung über Systeme hinweg misst, den Ausgleich von Lasten auf diesen Systemen unterstützen.

Das Monitoring-System umfasst zwei Komponenten: das Monitoring-System selbst, und den *Monitoring-Scout*. Das Monitoring-System ist im Satellite installiert und führt Backend-Funktionen durch, wie z.B. das Speichern von Monitoring-Daten und das Reagieren darauf. Der Monitoring-Scout führt alle Probes aus und sammelt Monitoring-Daten. Der Monitoring-Scout kann zum Betrieb auf einem Satellite- oder auf Red Hat Satellite Proxy-System konfiguriert werden. Der Einsatz von Monitoring-Scout auf Proxys erlaubt Ihnen, Arbeiten vom Satellite Server zu delegieren, wodurch Skalierbarkeit von Probes erreicht wird.

Monitoring umfasst das Festlegen von Benachrichtigungs-Methoden, die Installation von Probes auf Systemen, das regelmäßige Überprüfen des Status aller Probes sowie das Erstellen von Berichten, welche historische Daten für ein System oder einen Dienst anzeigen. In diesem Abschnitt wird versucht, die allgemeinen Aufgaben in Zusammenhang mit der Monitoring-Berechtigung zu identifizieren. Beachten Sie, dass sämtliche Änderungen, die Ihre Monitoring-Infrastruktur beeinflussen, finalisiert werden müssen, indem Sie über die **`Scout-Konfig-Push`** Seite Ihre Konfiguration aktualisieren.

1.2.1. Voraussetzungen

Bevor Sie versuchen Red Hat Network Monitoring in Ihrer Infrastruktur zu implementieren, vergewissern Sie sich, dass alle dazu notwendigen Tools vorhanden sind. Sie benötigen mindestens:

- Monitoring-Berechtigungen - Diese Berechtigungen sind für alle Systeme erforderlich, die überwacht werden sollen. Monitoring wird nur auf Red Hat Enterprise Linux Systemen unterstützt.
- Red Hat Satellite mit Monitoring - Monitoring-Systeme müssen mit einem Satellite verbunden sein, auf dem das Basisbetriebssystem Red Hat Enterprise Linux 5 oder später läuft.

- Monitoring-Administrator - Diese Rolle muss an Benutzer vergeben werden, die Probes installieren, Benachrichtigungsmethoden festlegen oder die Monitoring-Infrastruktur in irgendeiner Art verändern. (Bitte beachten Sie, dass der Satellite-Administrator automatisch die Fähigkeiten aller anderen Rollen/Funktionen innerhalb einer Organisation übernimmt und deshalb diese Aufgaben ausführen kann.) Vergeben Sie diese Rolle mittels der **Benutzerdetails** Seite für den Anwender.
- Red Hat Network Monitoring-Daemon - Dieser Daemon ist gemeinsam mit dem SSH-Schlüssel für den Scout auf Systemen erforderlich, die überwacht werden, damit die internen Prozess-Monitore ausgeführt werden können. Sie können diese Probes unter Umständen jedoch auch unter Verwendung des bestehenden SSH-Daemons (**sshd**) ausführen. Siehe Abschnitt 1.2.2, „Konfigurieren des Red Hat Network Monitoring Daemon (**rhnmd**)“ für Installationshinweise und für eine Liste von Probes, welche diese sichere Verbindung erfordern. Siehe Anhang A, *Probes* für eine vollständige Liste der verfügbaren Probes.

Monitoring aktivieren

Monitoring ist standardmäßig deaktiviert, Sie müssen es daher explizit aktivieren, bevor Sie es einsetzen können.

1. Melden Sie sich als Benutzer mit Satellite-Administrator-Rechten an und gehen Sie zu **Admin** → **Red Hat Satellite Konfiguration**. Klicken Sie das **Monitoring Aktivieren**Kontrollkästchen, dann **Aktualisieren** klicken, um die Änderung zu übernehmen.
2. Starten Sie die Dienste neu, damit die Änderungen wirksam werden. Klicken Sie auf den **Neustart** Tab, um den Satellite neu zu starten. Der Satellite wird dadurch für einige Minuten offline sein.
3. Überprüfen Sie, ob der **Monitoring** Tab unter **Red Hat Satellite Konfiguration** verfügbar ist um zu bestätigen, dass die Überwachung aktiviert ist.
4. Gehen Sie zu **Admin** → **Red Hat Satellite Konfiguration** → **Monitoring**. Klicken Sie das **Monitoring-Scout Aktivieren** Kontrollkästchen um den Scout zu aktivieren. Klicken Sie zum Speichern auf **Konfig aktualisieren**.

Anmerkung

Wir empfehlen Ihnen, die Monitoring-Konfigurationswerte auf ihren Standardwerten zu belassen. **Sendmail** muss konfiguriert werden, um Benachrichtigungen zu verwenden.

1.2.2. Konfigurieren des Red Hat Network Monitoring Daemon (rhnmd)

Um das Meiste aus Ihrer Monitoring-Berechtigung herauszuholen, empfiehlt Red Hat die Installation des Red Hat Network Monitoring-Daemons auf Ihren Client-Systemen. Basierend auf **OpenSSH** ermöglicht **rhnmd** dem Satellite, sicher mit dem Client-System zu kommunizieren, um auf interne Prozesse zugreifen und den Untersuchungs-Status abfragen zu können.

Bitte beachten Sie, dass der Red Hat Network Monitoring-Daemon von Systemen voraussetzt, dass diese Verbindungen zum Port 4545 zulassen. Sie können es vermeiden, diesen Port zu öffnen und den Daemon zu installieren, indem Sie stattdessen **sshd** verwenden. Siehe Abschnitt 1.2.2.2, „Konfiguration von SSH“ für Details.

Einige Probes erfordern den Dämon. Eine verschlüsselte Verbindung, entweder durch den Red Hat Network Monitoring Daemon oder **sshd**, ist auf Client-Systemen erforderlich, um folgende Probes auszuführen:

- Linux::CPU Usage
- Linux::Disk IO Throughput

- Linux::Disk Usage
- Linux::Inodes
- Linux::Interface Traffic
- Linux::Load
- Linux::Memory Usage
- Linux::Process Counts by State
- Linux::Process Count Total
- Linux::Process Health
- Linux::Process Running
- Linux::Swap Usage
- Linux::TCP Connections by State
- Linux::Users
- Linux::Virtual Memory
- LogAgent::Log Pattern Match
- LogAgent::Log Size
- Network Services::Remote Ping
- Oracle::Client Connectivity
- General::Remote Program
- General::Remote Program with Data

Beachten Sie, dass alle Probes der Linux-Gruppe diese Anforderung haben.

1.2.2.1. Installation des Red Hat Network Monitoring-Daemons

Installieren Sie den Red Hat Network Monitoring-Daemon, um Systeme auf das Monitoring unter Verwendung der Probes vorzubereiten, die in **`rhnmd`** festgelegt sind. Beachten Sie bitte, dass die Schritte in diesem Abschnitt optional sind falls Sie vorhaben sollten **sshd** zu verwenden, um sichere Verbindungen zwischen der Red Hat Monitoring-Infrastruktur und den überwachten Systemen zu ermöglichen. Siehe Abschnitt 1.2.2.2, „Konfiguration von SSH“ für Instruktionen.

Das **`rhnmd`** Paket befindet sich im Red Hat Network Tools-Channel für alle Red Hat Enterprise Linux Distributionen. Um es zu installieren:

1. Subskribieren Sie für die zu überwachenden Systeme den Red Hat Network Tools-Channel der dem System zugeordnet ist. Dies kann individuell mittels dem **System Details** → **Channels** → **Software** Unter-Tab oder für mehrere Systeme auf einmal mittels dem **Channel Details** → **Target Systems** Tab durchgeführt werden.
2. Sobald Sie subskribiert sind, öffnen Sie den **Channel Details** → **Packages** Tab und suchen das **`rhnmd`** Paket (unter 'R').
3. Klicken Sie den Paketnamen, um die **`Paket-Details`** Seite zu öffnen. Gehen Sie zum **`Zielsysteme`** Tab, wählen die gewünschten Systeme aus und klicken auf **`Pakete installieren`**.
4. Installieren Sie den öffentlichen SSH-Schlüssel auf allen Client-Systemen, die überwacht werden sollen, wie im Abschnitt 1.2.2.3, „Installation des SSH-Schlüssels“ beschrieben.
5. Starten Sie den Red Hat Network Monitoring-Daemon auf allen Client-Systemen mit dem Befehl:

   ```
   service rhnmd start
   ```

6. Wenn Sie Probes hinzufügen, die den Daemon erfordern, übernehmen Sie die Standardwerte für

RHNMD-Benutzer und **RHNMD-Port**: **nocpulse**, bzw. **4545**.

1.2.2.2. Konfiguration von SSH

Wenn Sie vermeiden möchten, den Red Hat Network Monitoring-Daemon zu installieren und den Port 4545 auf Client-Systemen zu öffnen, können Sie stattdessen **sshd** konfigurieren, um die verschlüsselte Verbindung zwischen den Systemen und Red Hat Network bereitzustellen. Dies kann insbesondere dann gewünscht sein, wenn **sshd** sowieso bereits läuft. Um den Daemon für die Monitoring-Verwendung zu konfigurieren:

1. Stellen Sie sicher, dass das SSH-Paket auf den zu überwachenden Systemen installiert ist.

```
rpm -qi openssh-server
```

2. Legen Sie den Benutzer fest, der mit dem Daemon verknüpft wird. Dies kann jeder auf dem System verfügbare Benutzer sein, solange der erforderliche SSH-Schlüssel in der **~/.ssh/authorized_keys** Datei des Benutzers abgelegt werden kann.
3. Legen Sie den vom Daemon benutzten Port fest, wie in der Konfigurationsdatei **/etc/ssh/sshd_config** festgelegt. Der Standard-Port ist 22.
4. Installieren Sie den öffentlichen SSH-Schlüssel auf allen Client-Systemen, die überwacht werden sollen, wie im Abschnitt 1.2.2.3, „Installation des SSH-Schlüssels“ beschrieben.
5. Starten Sie **sshd** auf allen Client-Systemen mit dem Befehl:

```
service sshd start
```

6. Wenn Sie Probes hinzufügen, die den Daemon erfordern, geben Sie die aus Schritt 2 und Schritt 3 abgeleiteten Werte in die Felder **RHNMD-User** und **RHNMD-Port** ein.

1.2.2.3. Installation des SSH-Schlüssels

Egal, ob Sie nun **rhnmd** oder **sshd** verwenden - Sie müssen den öffentlichen SSH-Schlüssel des Red Hat Network Monitoring-Daemons auf den zu überwachenden Systemen installieren, um die sichere Verbindung zu vervollständigen. Um den Schlüssel zu installieren:

1. Gehen Sie zur **Monitoring** → **Scout Config Push** Seite auf dem Satellite Interface und klicken Sie auf den Namen des Scouts, der das Client-System überwachen wird. Auf der daraufhin erscheinenden Seite sehen Sie den SSH **id_dsa.pub** Schlüssel.
2. Kopieren Sie den Zeichenstring (beginnend mit ssh-dss und mit dem Hostnamen des Satellite am Ende).
3. Klicken Sie auf **Systeme** auf dem Menü links und markieren Sie das Auswahlkästchen der Systeme, an die Sie den SSH-Schlüssel senden möchten. Klicken Sie oben auf der Seite auf den Link **Verwalten**, um den Vorgang abzuschließen.
4. Im **System Set Manager**, klicken Sie auf **Remote-Befehle ausführen**, und geben Sie anschließend im **Skript** Textfeld die folgende Zeile ein:

```
#!/bin/sh
cat <<EOF >> ~nocpulse/.ssh/authorized_keys
```

Drücken Sie danach die **Eingabe** Taste, fügen den SSH-Schlüssel ein und hängen EOF an. Das Ergebnis sollte etwa wie folgt aussehen:

```
#!/bin/sh
cat <<EOF>> ~nocpulse/.ssh/authorized_keys
ssh-dss AABBAB3NzaC3kc3MABCCBAJ4cmyf5jt/ihdtFbNE1YHsT0np0SYJz7xk
hzoKUUWnZmOUqJ7eXoTbGEcZjZLppOZgzAepw1vUHXfa/L9XiXvsV8K5Qmcu70h0
1gohBIder/1I1QbHMCgfDVFPtfV5eedau4AAACAc99dHbWhk/dMPiWXgHxdI0vT2
SnuozIox2klmfbTeO4Ajn/Ecfxqgs5diat/NIaeoItuGUYepXFoVv8DVL3wpp45E
02hjmp4j2MYNpc6Pc3nPOVntu6YBv+whB0VrsVzeqX89u23FFjTLGbfYrmMQflNi
j8yynGRePIMFhI= root@satellite.example.com
EOF
```

5. Legen Sie das Datum und die Uhrzeit fest, wann die Aktion durchgeführt werden soll, und klicken Sie anschließend auf **`Remote-Befehl einplanen`**.

Sobald der Schlüssel platziert wurde und zugänglich ist, sollten alle Probes, die diesen Schlüssel benötigen, **ssh** Verbindungen zwischen der Monitoring-Infrastruktur und dem überwachten System zulassen. Sie können dann damit beginnen, Probes, die den Monitoring-Daemon benötigen, auf den neu konfigurierten Systemen laufen zu lassen.

1.2.3. Konfigurieren des `mysql` Paketes für Probes

Wenn Ihr Red Hat Satellite Monitoring-berechtigten Client-Systemen dient, auf denen Sie **MySQL** Probes laufen lassen möchten, müssen Sie das **`mysql`** Paket auf dem Red Hat Satellite konfigurieren. Siehe Anhang A, *Probes* für eine Liste aller verfügbaren Probes.

Subskribieren Sie den Satellite zum Red Hat Enterprise Linux Basis-Channel und installieren das **`mysql`** Paket entweder mittels **`up2date`**, **`yum`** oder Red Hat Network Hosted.

Ist das abgeschlossen, kann Ihr Satellite nun dazu verwendet werden, MySQL-Probes laufen zu lassen.

1.2.4. Aktivieren Benachrichtigungen

Zusätzlich zur Ansicht des Probe-Status auf dem Red Hat Network Interface können Sie auch benachrichtigt werden, wann immer eine Probe den Status ändert. Dies ist von besonderer Wichtigkeit, wenn unternehmenskritische Produktionssysteme überwacht werden. Aus diesem Grund empfiehlt Red Hat, dieses Feature zu verwenden.

Um Probe-Benachrichtigungen in Red Hat Network zu aktivieren, müssen Sie einen Mail-Exchange-Server und eine Mail-Domain während Ihrer Red Hat Satellite Installation festgelegt haben und **`sendmail`** dahingehend konfiguriert haben, mit eingehenden Nachrichten richtig umzugehen. Für nähere Details siehe den Abschnitt *Installation* im *Red Hat Satellite Installationshandbuch*.

1.2.4.1. Erstellen von Benachrichtigungsmethoden

Benachrichtigungen werden via einer *Benachrichtigungsmethode* versendet – eine E-Mail- oder Pager-Adresse, die mit einem bestimmten Red Hat Network Benutzer verknüpft ist. Obwohl die Adresse mit einem bestimmten Benutzer-Account verknüpft ist, kann diese mittels einem Alias oder einer Mailingliste auch mehreren Administratoren dienen. Jeder Benutzer-Account kann mehrere Benachrichtigungs-Methoden enthalten. Um eine Benachrichtigungs-Methode anzulegen:

1. Melden Sie sich auf Satellite entweder als ein Satellite-Administrator oder Monitoring-Administrator an.
2. Gehen Sie zu **`Users`** und wählen den Benutzernamen aus. Auf der **`User Details`** Seite, klicken Sie auf **Notification Methods → `create new method`**.
3. Geben Sie ein intuitives, beschreibendes Label für den Namen der Methode ein, wie beispielsweise **`DBA E-Mail tagsüber`** und geben Sie die richtige E-Mail-Adresse ein. Denken Sie daran, dass die Labels für alle Benachrichtigungs-Methoden während der Probe-Erstellung in

einer einzigen Liste angezeigt werden, und diese Labels daher eindeutig in Ihrer Organisation sein sollten.

4. Wählen Sie das Kontrollkästchen aus, um gekürzte Mitteilungen an die E-Mail-Adresse gesendet zu bekommen. Dieses kürzere Format beinhaltet lediglich den Probe-Status, den System-Hostnamen, Probe-Namen, den Zeitpunkt der Mitteilung und die Sende-ID. Das standardmäßige, längere Format zeigt zusätzlich einen Nachrichtenkopf, System- und Probe-Details und Anleitungen für eine Rückantwort an.
5. Wenn Sie fertig sind, klicken Sie auf **`Methode erstellen`**. Die neue Methode erscheint in **User Details → Notification Methods** Tab und auf der **`Benachrichtigung`** Seite unter der obersten **`Monitoring`** Kategorie. Klicken Sie auf den Namen, um sie zu bearbeiten oder zu löschen.
6. Während Sie Probes hinzufügen, wählen Sie das **`Probe-Benachrichtigungen`** Auswahlkästchen aus und wählen Sie die neue Benachrichtigungs-Methode vom daraus resultierenden Auswahl-Menü aus. Benachrichtigungs-Methoden, die Probes zugeordnet sind, können nur dann gelöscht werden, wenn sie von der Probe getrennt sind.

1.2.4.2. Erhalten von Benachrichtigungen

Wenn Sie Benachrichtigungs-Methoden anlegen und diese mit Probes verknüpfen, müssen Sie auch darauf vorbereitet sein, diese zu erhalten. Sie erhalten diese Benachrichtigungen in Form von kurzen Textmitteilungen, die an die spefizierte E-Mail-Adresse gesendet werden. Hier ist ein Beispiel einer E-Mail-Benachrichtigung:

```
Subject: CRITICAL: [hostname]: Satellite: Users at 1
From: "Monitoring Satellite Notification" (rogerthat01@redhat.com)
Date: Mon, 26 Aug 2013 13:42:28 -0800
To: user@organization.com

This is Red Hat Monitoring Satellite notification 01dc8hqw.

Time: Mon Aug 26, 21:42:25 PST
State: CRITICAL
System: [hostname] ([IP address])
Probe: Satellite: Users
Message: Users 6 (above critical threshold of 2)
Notification #116 for Users

Run from: Red Hat Monitoring Satellite
```

Wie Sie sehen, enthalten die längeren E-Mail-Benachrichtigungen so gut wie alles, was Sie über den damit verbundenen Probe wissen müssen. Zusätzlich zum Probe-Befehl, der Laufzeit, dem überwachten System und dem Status beinhaltet die Nachricht die *Sende-ID*, welche eine einzigartige Zeichenfolge ist. In der oben angeführten Mitteilung ist die Sende-ID 01dc8hqw.

Anmerkung

Da Benachrichtigungen immer dann generiert werden können, wenn ein Probe den Status wechselt, können einfachste Veränderungen in Ihrem Netzwerk in einer Flut von Benachrichtigungen resultieren. Benachrichtigungen können zu einer bestimmten Inbox für Benachrichtigungen umgeleitet werden um Probleme mit Prioritäts-Mail zu vermeiden. Umgeleitete Benachrichtigungen sind Gegenstand des nächsten Abschnitts.

1.2.4.3. Umleiten von Benachrichtigungen

Auf den Erhalt einer Benachrichtigung hin können Sie diese umleiten, indem Sie erweiterte Benachrichtigungs-Regeln in eine Bestätigungs-E-Mail einfügen. Aktivieren Sie die E-Mail-Umleitungen, indem Sie **/etc/aliases** öffnen und die folgende Zeile hinzufügen.

```
rogerthat01:    "| /etc/smrsh/ack_queuer.pl"
```

Nachdem Sie den Parameter eingestellt haben, antworten Sie auf die Benachrichtigungs-E-Mail und fügen Sie die gewünschte Option hinzu. Dies sind die möglichen Optionen, auch *Filtertypen* genannt:

- ACK METOO - Sendet die Benachrichtigung an das Umleitungsziel, sowie *zusätzlich* an das standardmäßige Ziel.
- ACK SUSPEND - Setzt die Benachrichtigungs-Methode für einen angegebenen Zeitraum aus.
- ACK AUTOACK - Ändert nicht das Ziel der Benachrichtigung, erkennt jedoch automatisch zusammenpassende Warnhinweise, sobald diese gesendet werden.
- ACK REDIR - Sendet die Benachrichtigung an das Umleitungsziel, *anstatt* an das standardmäßige Ziel.

Das Format der Regel sollte ***filter_type probe_type duration email_address*** sein, wobei ***filter_type*** einen der vorangehenden erweiterten Befehle darstellt, ***probe_type*** für **check** oder **host** steht, ***duration*** für die Dauer der Umleitung und ***email_address*** für den beabsichtigten Empfänger steht. Zum Beispiel:

```
ACK METOO host 1h boss@domain.com
```

Großschreibung ist nicht erforderlich. Die Dauer kann in Minuten (m), Stunden (h) oder Tagen (d) angegeben werden. E-Mail-Adressen werden nur für umgeleitete (REDIR) Benachrichtigungen und zusätzliche (METOO) Benachrichtigungen benötigt.

Die Beschreibung der Aktion, die in der daraus resultierenden E-Mail enthalten ist, ist standardmäßig der vom Benutzer eingegebene Befehl. Der aufgelistete Grund ist eine Zusammenfassung der Aktion, wie z.B. email ack redirect by user@domain.com, wobei user der Sender der E-Mail ist.

Anmerkung

Sie können beinahe alle Probe-Benachrichtigungen anhalten oder umleiten, indem Sie auf eine Benachrichtigungs-E-Mail mit einer Variation des Befehls **ack suspend host** antworten. Sie können jedoch keine Satellite Probe-Benachrichtigungen anhalten, indem Sie auf die Probe mit **ack suspend host** antworten oder Antworten umleiten. Bei diesen Probes müssen Sie die Benachrichtigungen auf der Satellite-Weboberfläche umändern.

1.2.4.4. Löschen von Benachrichtigungsmethoden

Vorhandene Beziehungen zwischen Methoden und Probes können den Vorgang der Entfernung von Benachrichtigungs-Methoden erschweren. Führen Sie die folgenden Schritte aus, um eine Benachrichtigungs-Methode zu löschen:

1. Melden Sie sich auf Satellite als ein Satellite-Administrator oder Monitoring-Administrator an.
2. Gehen Sie zur **Monitoring** → **Notifications** Seite und klicken Sie auf den Namen der Methode, die entfernt werden soll.
3. Auf dem **User** → **User Details** → **Notification Methods** Tab klicken Sie **Methode löschen**. Wenn die Methode nicht mit irgendwelchen Probes in Beziehung steht, erhalten Sie eine

Bestätigungsseite. Klicken Sie **Löschen bestätigen**. Die Benachrichtigungs-Methode wird entfernt.

Anmerkung

Da sowohl Name als auch Adresse der Benachrichtigungs-Methode bearbeitet werden können, sollten Sie lieber das Aktualisieren der Methode erwägen, als das Löschen. Dadurch werden Benachrichtigungen aller Probes, die diese Methode nutzen, umgeleitet, ohne dass jede Probe eigens bearbeitet und eine neue Benachrichtigungs-Methode angelegt werden muss.

4. Wenn die Methode mit einem oder mit mehreren Probes verknüpft ist, dann erhalten Sie anstelle der Bestätigungsseite eine Liste der Probes, die diese Methode verwenden sowie die damit verknüpften Systeme. Klicken Sie den Probe-Namen, um direkt zum **System Details → Probes** Tab zu gelangen.
5. Wählen Sie eine andere Benachrichtigungs-Methode aus und klicken Sie **Probe aktualisieren**.
6. Sie können nun zur **Monitoring → Notifications** Seite zurückkehren und die Benachrichtigungs-Methode löschen.

1.2.5. Über Probes

Nun, da der Red Hatwork Monitoring-Daemon installiert ist und Benachrichtigungs-Methoden angelegt worden sind, können Sie mit dem Installieren von Probes auf Ihren Monitoring-berechtigten Systemen beginnen. Wenn ein System eine Berechtigung für Monitoring besitzt, erscheint ein **Probes** Tab auf dessen **System-Details** Seite. Hier werden Sie die meisten Aufgaben im Zusammenhang mit Probes durchführen.

1.2.5.1. Verwalten von Probes

Die Probes werden durch den Red Hat Satellite Server erstellt. Sobald die Probe erstellt wurde, werden die Probes auf die angegebenen Monitoring-berechtigten Systeme, die auf dem Satellite registriert sind, propagiert. Gehen Sie folgendermaßen vor, um eine Probe im Satellite Server hinzuzufügen:

1. Melden Sie sich auf Satellite entweder als Satellite-Administrator oder als Systemgruppen-Administrator für das System an.
2. Gehen Sie zum **System Details → Probes** Tab und klicken Sie **Neue Probe anlegen**.
3. Füllen Sie auf der **System-Probe-Erstellung** Seite alle erforderlichen Felder aus. Wählen Sie zuerst die Probe-Befehlsgruppe. Dies ändert die Liste verfügbarer Probes und anderer Felder und Anforderungen. Siehe Anhang A, *Probes* für die komplette Liste von Probes nach Befehlsgruppe gegliedert. Beachten Sie, dass für einige Probes der Red Hat Network Monitoring-Daemon auf dem Client-System installiert sein muss.
4. Wählen Sie den gewünschten Probe-Befehl und den Monitoring-Scout, normalerweise **Red Hat Monitoring Satellite**, aber unter Umständen auch einen Red Hat Satellite Proxy Server. Geben Sie eine kurze und eindeutige Beschreibung für die Probe ein.
5. Markieren Sie das Auswahlkästchen **Probe-Benachrichtigungen**, um Benachrichtigungen zu erhalten, sobald die Probe ihren Status ändert. Benutzen Sie das **Probe-Testintervall** Auswahl-Menü, um festzulegen, wie oft Benachrichtigungen gesendet werden sollen. Wenn Sie **1 Minute** auswählen (und das Auswahlkästchen **Probe-Benachrichtigung**), bedeutet dies, dass Sie jede Minute eine Benachrichtigung erhalten, sobald die Probe deren KRITISCH- oder WARNUNG-Grenzwert übersteigt. Siehe Abschnitt 1.2.4, „Aktivieren Benachrichtigungen“ um herauszufinden, wie Benachrichtigungs-Methoden angelegt werden können und wie Sie deren

Empfang bestätigen können.

6. Benutzen Sie die **RHNMD Benutzer**- und **RHNMD Port** Felder, falls diese erscheinen, um die Probe zur Kommunikation via **sshd** und nicht via dem Red Hat Network Monitoring-Daemon zu zwingen. Siehe Abschnitt 1.2.2.2, „Konfiguration von SSH“ für nähere Details. Übernehmen Sie andernfalls die Standardwerte **nocpulse** bzw. **4545**.
7. Wenn das **Timeout** Feld erscheint, überprüfen Sie den Standardwert und passen ihn ggf. Ihren Bedürfnissen an. Die meisten Timeouts, jedoch nicht alle, haben den Status UNBEKANNT zur Folge. Wenn die Metriken der Probes auf Zeit basieren, dann gehen Sie sicher, dass die Timeout-Periode nicht kürzer als die Zeitspanne ist, die für die Grenzwerte festgelegt wurde. Ansonsten erfüllen die Metriken keinen Zweck, da die Probe durch das Timeout unterbrochen wird, bevor noch irgendwelche Grenzwerte überschritten werden können.
8. Benutzen Sie die verbleibenden Felder dazu, die Warngrenzwerte der Probe festzulegen, sofern zutreffend. Diese KRITISCH- und WARNUNG-Werte legen fest, an welchem Punkt die Probe ihren Status ändert. Siehe Abschnitt 1.2.5.2, „Festlegen von Grenzwerten“ für die optimalen Verfahrensweisen in Bezug auf diese Grenzwerte.
9. Klicken Sie zum Abschluss auf **Probe erstellen**. Vergessen Sie nicht, Ihre Monitoring-Konfigurationsänderung auf der **Scout-Konfig-Push** Seite einzureichen, damit die Aktualisierung wirksam wird.

Um eine Probe zu löschen, gehen Sie zur **Aktueller Status** Seite (indem Sie auf den Namen des Probe vom **System Details → Probes** Tab klicken) und klicken auf **Probe löschen**. Bestätigen Sie anschließend den Löschvorgang.

1.2.5.2. Festlegen von Grenzwerten

Viele der von Red Hat Satellite angebotenen Probes beinhalten Warngrenzwerte, die bei deren Überschreitung eine Statusänderung für die Probe anzeigen. Beispielsweise ermöglicht die Linux::CPU Usage Probe, die Grenzwerte KRITISCH und WARNUNG für den Prozentsatz an verwendeter CPU zu setzen. Wenn das überwachte System eine CPU-Gesamtnutzung von 75 Prozent meldet und der WARNUNG-Grenzwert auf 70 Prozent gesetzt ist, wird die Probe in einen WARNUNG-Status übergehen. Einige Probes bieten eine Vielzahl solcher Grenzwerte an.

Um das meiste aus Ihrer Monitoring-Berechtigung herauszuholen und falsche Benachrichtigungen zu vermeiden, empfiehlt Red Hat, die Probes für eine gewisse Zeit lang ohne Benachrichtigungen laufen zu lassen, um ein Basisverhalten für jedes Ihrer Systeme zu bestimmen. Obwohl sich die Standardwerte für Probes für Ihre Zwecke eignen können, so hat jede Organisation eine unterschiedliche Umgebung, die eventuell das Abändern der Grenzwerte erforderlich macht.

1.2.5.3. Überwachung des Satellite Servers

Zusätzlich zur Überwachung aller Ihrer Client-Systeme können Sie Red Hat Network auch dazu verwenden, Ihren Satellite oder Proxy zu überwachen. Um Ihren Satellite oder Proxy zu überwachen, suchen Sie ein System, das vom Server überwacht wird und gehen Sie zum **System Details → Probes** Tab dieses Systems.

Klicken Sie **Neue Probe erstellen** und wählen die **Satellite** Probe-Befehlsgruppe aus. Füllen Sie danach die anderen Felder aus, wie Sie dies auch für jede andere Probe tun würden. Siehe Abschnitt 1.2.5.1, „Verwalten von Probes“ für Instruktionen.

Obwohl es so aussieht, als ob der Satellite oder Proxy vom Client-System überwacht wird, wird die Probe eigentlich vom Server selbst ausgeführt. Grenzwerte und Benachrichtigungen funktionieren wie gewohnt.

Anmerkung

Sämtliche Probes, die Red Hat Network Monitoring-Daemon-Verbindungen benötigen, können nicht auf einem Red Hat Satellite oder Red Hat Satellite Proxy Server angewendet werden, auf dem Monitoring-Software läuft. Dies trifft auf die meisten Probes in der Linux-Befehlsgruppe zu sowie auch auf die Log-Agent-Probes und die Remote-Program-Probes. Verwenden Sie die Probes der Satellite-Befehlsgruppe, um Red Hat Satellite und Red Hat Satellite Proxy Server zu überwachen. Für Proxy-Scouts finden Sie die Probes unter dem System aufgelistet, für das sie Daten berichten.

1.2.6. Monitoring

Wenn Sie auf den **Monitoring** Tab auf der oberen Navigationsleiste klicken, erscheint die **Monitoring** Kategorie samt Links. Diese Seiten, für die Monitoring-Berechtigungen erforderlich sind, zeigen Ihnen die Resultate von Probes an, die auf Systemen mit Monitoring-Berechtigungen ausgeführt worden sind und ermöglichen es Ihnen, die Konfiguration Ihrer Monitoring-Infrastruktur zu verwalten.

Veranlassen Sie die Überwachung eines Systems auf dem **Probes** Tab der **System-Details** Seite. Siehe Anhang A, *Probes* für die vollständige Liste verfügbarer Probes.

1.2.6.1. Probe-Status

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Die **Probe-Status** Seite wird standardmäßig angezeigt, sobald Sie auf **Monitoring** in der oberen Navigationsleiste klicken.

Die **Probe-Status** Seite zeigt die Gesamtanzahl der Probes in den unterschiedlichen Status an und bietet eine einfache Oberfläche, um problematische Probes schnell auffinden zu können. Beachten Sie, dass die Gesamtanzahl von Probes in den Tabs oben auf der Seite eventuell nicht der Anzahl von Probes in den darunter stehenden Tabellen entspricht. Die Werte oben beinhalten Probes für alle Systeme in Ihrer Organisation, wogegen die Tabellen lediglich Probes für die Systeme anzeigen, zu denen Sie durch Ihre Rolle als Systemgruppen-Administrator Zugang haben. Zudem werden die hier angezeigten Probe-Anzahlen um bis zu eine Minute verzögert aktualisiert.

Die folgende Liste beschreibt jeden Status und die damit verbundenen Symbole:

- - *Kritisch* - Die Probe hat den KRITISCH-Grenzwert überschritten.
- - *Warnung* - Die Probe hat den WARNUNG-Grenzwert überschritten.
- - *Unbekannt* - Die Probe ist unfähig, Messdaten oder Status-Informationen korrekt zu berichten.
- - *Ausstehend* - Die Probe wurde geplant, lief aber bisher nicht, bzw. ist nicht in der Lage zu laufen.
- - *OK* - Die Probe wird erfolgreich ausgeführt.

Die **Probe-Status** Seite beinhaltet Tabs für jeden möglichen Status sowie einen Tab, der alle Probes auflistet. Jede Tabelle enthält Spalten, in denen der Probe-Status, das überwachte System, die eingesetzten Probes, sowie Datum und Uhrzeit der letzten Status-Aktualisierung angezeigt werden.

In diesen Tabellen gelangen Sie durch einen Klick auf den Systemnamen zum **Monitoring** Tab auf der **System-Details** Seite. Durch einen Klick auf den Namen einer Probe gelangen Sie zu deren **Aktueller Status** Seite. Von hier aus können Sie die Probe bearbeiten, löschen und Berichte basierend auf ihren Ergebnissen erstellen.

Monitoring-Daten und Probe-Status-Informationen, die bisher nur über die Weboberfläche des Satellites verfügbar waren, können nun als CSV-Datei exportiert werden. Klicken Sie auf die Verknüpfung **CVS Herunterladen** auf den Monitoring-Seiten, um CSV-Dateien mit relevanten Informationen herunterzuladen. Die exportierten Daten können u.a. folgendes beinhalten:

- Probe-Status
- Alle Probes in einem vorgegebenen Status (OK, WARNUNG, UNBEKANNT, KRITISCH, AUSSTEHEND)
- Ein Probe-Ereignisverlauf

1.2.6.1.1. Probe-Status ⇒ Kritisch

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Diese Probes haben ihre KRITISCH-Grenzwerte überschritten oder sind aus anderen Gründen in einen kritischen Status übergegangen. Manche Probes gehen in den Status KRITISCH über, wenn ihr Timeout-Wert überschritten wurde.)

1.2.6.1.2. Probe-Status ⇒ Warnung

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Probes, die ihre WARNUNG-Grenzwerte überschritten haben.

1.2.6.1.3. Probe-Status ⇒ Unbekannt

Wichtig

Die Monitoring-Berechtigung ist für diese Funktion erforderlich.

Probes, die nicht die notwendigen Metriken sammeln können, um einen Probe-Status ermitteln zu können. Die meisten Probes, wenn auch nicht alle, gehen in einen 'Unbekannt'-Status über, wenn ihr Timeout-Wert überschritten wird. Dies kann bedeuten, dass der Timeout-Wert angehoben werden sollte oder dass die Verbindung zum betreffenden System nicht hergestellt werden kann.

Es ist auch möglich, dass die Konfigurations-Parameter der Probes nicht stimmen und deren Daten daher nicht gefunden werden können. Schlussendlich kann dieser Status auch bedeuten, dass ein Softwarefehler aufgetreten ist.

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Die Probes, deren Daten noch nicht von Red Hat Network erhalten wurden. Dieser Status beschreibt eine Probe, die gerade eingeplant worden ist, aber noch nicht durchgeführt wurde. Wenn alle Probes in einen 'Ausstehend'-Status übergehen, kann es sein, dass Ihre Überwachungs-Infrastruktur fehlerhaft ist.

1.2.6.1.5. Probe-Status ⇒ OK

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Diese Probes sind erfolgreich ohne Fehler gelaufen. Dies ist der gewünschte Status für alle Probes.

1.2.6.1.6. Probe-Status ⇒ Alle

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Alle Probes, die für Systeme in Ihrem Account eingeplant sind, werden in alphabetischer Reihenfolge der Systemnamen gelistet.

1.2.6.1.7. Aktueller Status

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Zeigt den Status der ausgewählten Probe an und wann diese zuletzt ausgeführt wurde. Ein Bericht kann ebenfalls in Bezug auf diese Probe erstellt werden. Obwohl diese Seite Teil des Monitorings ist, befindet sie sich unter dem **`Probes`** Tab innerhalb der **`System-Details`** Seite, da deren Konfiguration spezifisch für das überwachte System ist.

Um einen Bericht über die Resultate der Probe zu erhalten, wählen Sie eine relevante Dauer mittels der **`Datum`** Felder aus und entscheiden, ob Sie Messdaten, die Status-Änderungsgeschichte oder beides sehen möchten. Um Messdaten zu erhalten, wählen Sie die Metrik(en) aus, über die Sie einen Bericht erhalten möchten. Wählen Sie des weiteren mit den Auswahlkästchen, ob Sie die Resultate in Form eines Diagramms, eines Fehlerprotokolls oder beides gleichzeitig möchten. Klicken Sie dann **`Bericht erstellen`** ganz unten auf der Seite. Wenn es keine Daten für die festgesetzten Metriken gibt, erscheint folgende Meldung: NO DATA FOR SELECTED TIME PERIOD AND METRIC (Keine Daten wurden für den festgelegten Zeitraum und die Metriken gefunden).

1.2.6.2. Benachrichtigung

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Zeigt die Kontaktmethoden an, die für Ihre Organisation festgelegt wurden. Diese Methoden beinhalten E-Mail- oder Pager-Adressen, die dazu bestimmt sind, Warnmeldungen von Probes zu erhalten.

Die unterschiedlichen Benachrichtigungs-Methoden, die Ihrer Organisation zur Verfügung stehen, sind hier auf dem Standardbildschirm **`Benachrichtigungen`** ersichtlich. Die Methoden sind in Bezug auf den Benutzer aufgelistet, auf den diese zutreffen.

Um eine neue Benachrichtigungs-Methode anzulegen, klicken Sie auf den Namen des Benutzers, an den die Benachrichtigungen gerichtet sein sollen. Die entsprechende Seite Benutzerdetails ⇒ Benachrichtigungs-Methoden erscheint. Klicken Sie auf den Titel der Benachrichtigungs-Methode, um die Eigenschaften der Methode zu bearbeiten.

1.2.6.2.1. Benachrichtigung ⇒ Filter

Benachrichtigungs-Filter ermöglichen es Ihnen, Langzeitregeln festzulegen, die Standard-Benachrichtigungen aussetzen, umleiten, automatisch deren Empfang bestätigen oder ergänzende Zusatznachrichten senden. Dies kann hilfreich bei der Verwaltung von ausführlicher oder häufiger Probes-Kommunikation sein.

1.2.6.2.1.1. Benachrichtigung ⇒ Benachrichtigungsfilter ⇒ Aktive Filter

Dies ist der Benachrichtigungs-Filter Tab. Alle aktiven Filter, die Ihrer Organisation zur Verfügung stehen, werden hier aufgelistet. Klicken Sie auf den Namen des Filters, um dessen Eigenschaften zu bearbeiten.

Um einen Benachrichtigungs-Filter zu erstellen, klicken Sie den Link **`Neuen Benachrichtigungs-Filter erstellen`** rechts oben auf dem Bildschirm. Konfigurieren Sie jede unten aufgeführte Option und klicken Sie die **`Filter speichern`** Schaltfläche, um den Filter zu erstellen.

1. *Beschreibung*: Geben Sie einen Wert ein, der es Ihnen ermöglicht, diesen Filter von allen anderen Filtern zu unterscheiden.
2. *Typ*: Legen Sie fest, welche Aktionen der Filter ausführen soll: Umleiten, Empfang bestätigen, Aussetzen oder die eingehende Benachrichtigung ergänzen.
3. *Senden an*: Die Optionen **`Benachrichtigung Umleiten`** und **`Ergänzende Benachrichtigung`** erfordern die Angabe einer E-Mail-Adresse. Die verbleibenden Optionen benötigen keine E-Mail-Adressangabe.
4. *Anwendungsbereich*: Legen Sie fest, welche Überwachungskomponenten gefiltert werden sollen.
5. *Organisation/Scout/Probe*: Diese Option ermöglicht es Ihnen, die Organisation, Scout(s) oder Probe(s) auszuwählen, auf die dieser Filter zutrifft. Halten Sie die **`Strg`**-Taste gedrückt, um mehrere Positionen gleichzeitig auswählen zu können. Halten Sie die **`Umschalt`**-Taste gedrückt, wenn Sie eine aufeinanderfolgende Reihe von Einträgen markieren möchten.
6. *Probes in Status*: Wählen Sie aus, welche Probe-Status sich auf den Filter beziehen. Beispielsweise können Sie festlegen, dass ergänzende Benachrichtigungen lediglich für kritische Probes erstellt werden sollen. Wenn Sie möchten, dass der Filter einen Status ignoriert, dann heben Sie die Auswahl des Kästchens links von jeweiligen Status auf.
7. *Benachrichtigungen gesendet an*: Dies ist die Methode, an welche die Benachrichtigung gesendet würde, wenn kein Filter vorhanden wäre. Sie können beispielsweise Benachrichtigungen, die normalerweise an einen Benutzer gesendet werden, umleiten, während dieser im Urlaub ist. Dabei

bleiben alle anderen Benachrichtigungen von dieser Probe unverändert.

8. *Übereinstimmung mit Ausgabe*: Wählen Sie präzise Benachrichtigungs-Resultate aus, indem Sie hier einen regulären Ausdruck eingeben. Wenn die Ausgabe der Benachrichtigung nicht dem regulären Ausdruck entspricht, dann findet der Filter keine Anwendung.
9. *Wiederholt*: Wählen Sie aus, ob ein Filter durchgehend oder wiederholt abläuft. Ein sich wiederholender Filter läuft mehrmals während einer bestimmten Zeitspanne ab, die geringer ist als die Dauer des Filters. Beispielsweise könnte ein sich wiederholender Filter jede Stunde 10 Minuten lang zwischen den Anfangs- und Endzeiten des Filters laufen. Ein sich nicht wiederholender Filter läuft ohne Unterbrechung zwischen den Start- und Endzeiten des Filters.
10. *Beginnt*: Geben Sie Datum und Uhrzeit für den Beginn des Einsatzes des Filters ein.
11. *Endet*: Geben Sie Enddatum und -zeit für den Filter ein.
12. *Dauer jeder Wiederholung*: Wie lange der sich wiederholende Filter aktiv ist. Dieses Feld, das nur bei sich wiederholenden Filtern ausgefüllt werden muss, beginnt zur oben angegebenen **`Beginnt`**-Zeit. Alle Benachrichtigungen, die außerhalb der festgelegten Zeiträume generiert werden, werden nicht gefiltert.
13. *Häufigkeit*: Wie oft der Filter aktiviert wird.

Benachrichtigungs-Filter können nicht gelöscht werden. Ein Filter kann jedoch beendet werden, indem das Enddatum auf ein Datum in der Vergangenheit gesetzt wird (dies darf nicht vor dem Startdatum liegen). Sie können auch ein Filter-Set von der **`Aktiv`** Seite auswählen und die Schaltfläche **`Benachrichtigungs-Filter Beenden`** rechts unten klicken. Diese Filter werden dann beendet und erscheinen im **`Abgelaufene Filter`** Tab.

1.2.6.2.1.2. Benachrichtigung ⇒ Benachrichtigungs-Filter ⇒ Abgelaufene Filter

Dieser Tab listet alle Benachrichtigungs-Ffilter, deren Enddatum überschritten wurde. Abgelaufene Filter werden auf unbegrenzte Zeit aufbewahrt; dies ermöglicht es einer Organisation, nützliche Filter bei Bedarf wiederzuverwenden und bildet gleichzeitig eine historische Aufzeichnung zur Problembehebung.

1.2.6.3. Probe-Suites

Probe-Suites ermöglichen es Ihnen, einen oder mehrere Probes auf einem System oder auf Systemen anzuwenden. Probe-Suites können einmal konfiguriert werden und dann auf einer beliebigen Anzahl von Systemen gleichzeitig angewendet werden, was Zeitersparnisse und verbesserte Übereinstimmung für Monitoring-Verwender ermöglicht.

Um eine Probe-Suite zu erstellen und anzuwenden, erstellen Sie zuerst eine leere Probe-Suite, konfigurieren dann die Mitglieds-Probes und wenden schlussendlich die Suite auf den ausgewählten Systemen an.

1. Auf der Monitoring ⇒ Probe-Suites Seite wählen Sie den Link **`Neue Probe-Suite erstellen`** aus. Geben Sie einen einfach zu unterscheidenden Namen ein. Sie können auch eine kurze Beschreibung der Suite eingeben. Klicken Sie die Schaltfläche **`Probe-Suite erstellen`**, um fortzufahren.
2. Sie müssen nun die Probes hinzufügen und konfigurieren, aus denen die Suite besteht. Klicken Sie den **`Neuen Probe erstellen`** Link ganz oben rechts.
3. Konfigurieren Sie die Probe und klicken Sie die **`Probe erstellen`** Schaltfläche rechts unten. Wiederholen Sie dies solange, bis alle gewünschten Probes hinzugefügt wurden.

Anmerkung

Sendmail muss richtig auf Ihrem Red Hat Satellite konfiguriert sein und auf jedem Client-System, auf dem die Probe-Suite angewendet wird, muss der **rhnmd** Daemon installiert sein und laufen. Siehe das *Red Hat Satellite Installationshandbuch* für zusätzliche Informationen.

4. Auf dem "Systems" Tab fügen Sie die Systeme hinzu, auf welche die Probe-Suite angewendet werden soll. Klicken Sie den Link **Systeme zur Probe-Suite hinzufügen** oben rechts auf dem Bildschirm, um fortzufahren.
5. Die nächste Seite zeigt eine Liste aller Systeme mit Monitoring-Berechtigung an. Markieren Sie das Kästchen links von den Systemen, die Sie mit der Probe-Suite verknüpfen möchten, wählen den Monitoring-Scout aus, den Sie verwenden möchten und klicken die Schaltfläche **Systeme zur Probe-Suite hinzufügen**, um die Erstellung der Probe-Suite abzuschließen.

Sie könne Probes entweder löschen oder von der Suite abtrennen. Das Abtrennen hat ein Auflösung der Verbindung der Probes mit der Suite zur Folge und wandelt diese in systemspezifische Probes um. Dies bedeutet, dass Veränderungen an den abgetrennten Probes nur dieses System betreffen. Das Löschen eines Probes entfernt diesen nachhaltig von der Suite.

Um Probes von der Probe-Suite zu entfernen:

1. Klicken Sie auf der Monitoring ⇒ Probe-Suites-Seite auf den Titel der Probe-Suite, die Sie ändern möchten.
2. Wählen Sie den **Probes** Sub-Tab aus.
3. Wählen Sie das Kästchen neben dem Probe aus, den Sie entfernen möchten.
4. Klicken Sie die Schaltfläche **Probes von Probe-Suites löschen**.

Sie können auch ein System von der Probe-Suite entfernen. Sie können dies auf zwei Arten tun. Sie können erstens das System von der Probe-Suite abtrennen. In diesem Fall sind immer noch dieselben Probes mit dem System verknüpft. Sie haben jedoch nunmehr die Möglichkeit, diese Probes individuell zu konfigurieren, ohne dass dabei andere Systeme beeinträchtigt werden.

Systeme von der Suite abtrennen:

1. Auf der **Monitoring** ⇒ **Probe-Suites**-Seite klicken Sie auf den Titel der Probe-Suite, die Sie ändern möchten.
2. Wählen Sie den **Systeme** Sub-Tab aus.
3. Markieren Sie die Auswahlkästchen neben den Systemen, die Sie entfernen möchten.
4. Klicken Sie die Schaltfläche **System(e) von Probe-Suite abtrennen**.

Die zweite Methode ist das Entfernen des Systems von der Suite. Dies entfernt das System von der Suite und löscht alle Probes vom System.

Anmerkung

Dieser Vorgang löscht alle Probes der Probe-Suite auf dem System sowie auch alle historischen Time-Series und Ereignisprotokoll-Daten. Dieser Vorgang kann nicht rückgängig gemacht werden.

Um ein System von der Probe-Suite zu entfernen und alle damit verbunden Probes vom System zu löschen:

1. Klicken Sie auf der Monitoring ⇒ Probe-Suites-Seite auf den Titel der Probe-Suite, die Sie ändern möchten.
2. Wählen Sie den **`Systeme`** Sub-Tab aus.
3. Markieren Sie die Auswahlkästchen neben den Systemen, die Sie entfernen möchten.
4. Klicken Sie die Schaltfläche **`System(e) von Probe-Suite entfernen`**.

Abschließend können Sie, wie bei einzelnen Probes auch, eine CVS-Datei mit Informationen zur Probe-Suite herunterladen. Klicken Sie auf den Link **`CSV herunterladen`** am unteren Rand der Seite **`Monitoring`** ⇒ **`Probe-Suites`**, um die Datei herunterzuladen.

1.2.6.4. Scout Config Push

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Zeigt den Status Ihrer Monitoring-Infrastruktur an. Jedes mal, wenn Sie eine Änderung durchführen, wie z.B. das Hinzufügen eines Probes oder das Bearbeiten der Grenzwerte eines Probes, müssen Sie Ihre Monitoring-Infrastruktur rekonfigurieren. Wählen Sie dazu das Auswahlkästchen des Red Hat Network Servers aus und klicken Sie **`Push Scout-Konfigs`**. Die Tabelle auf dieser Seite zeigt Datum und Uhrzeit von angefragten und abgeschlossenen Push-Aktionen an.

Indem Sie den Namen des Servers anklicken, wird dessen öffentlicher SSH-Schlüssel des Red Hat Network Monitoring-Daemons geöffnet. Dies ermöglicht es Ihnen, den SSH-Schlüssel zu kopieren und für diejenigen Systeme einzufügen, die vom Scout überwacht werden. Dies ist erforderlich, damit der Red Hat Network Monitoring Daemon mit dem Satellite verbindet.

1.2.6.5. Allgemeine Monitoring-Konfiguration

Wichtig

Die Monitoring-Berechtigung ist erforderlich, um diesen Tab zu sehen.

Die Allgemeine Monitoring-Konfigurationsseite befindet sich in **Admin → Red Hat Satellite Configuration → Monitoring**. Sie sammelt Informationen, die universell auf Ihre Monitoring-Infrastruktur anwendbar sind. Wenn Sie irgendetwas auf dieser Seite modifizieren, werden infolgedessen die Monitoring-Dienste auf dem Red Hat Satellite zurückgesetzt. Ebenso werden sämtliche geplanten Aktionen für die Monitoring-Dienste auf allen Monitoring-fähigen Red Hat Satellite Proxy Servern, die zu diesem Satellite gehören, neu gestartet. Dadurch werden alle Monitoring-Dienste auf diesen Servern ihre Konfiguration umgehend neu laden.

Üblicherweise sind die Standardeinstellungen in anderen Feldern ausreichend, da diese von Ihrer Satellite-Installation abgeleitet sind. Dennoch können Sie die Felder auf dieser Seite dazu verwenden, Ihre Monitoring-Konfiguration zu verändern. Beispielsweise können Sie hier Ihren Mail-Server ändern. Diese Seite ermöglicht es Ihnen auch, die Zieladresse aller administrativen E-Mails zu ändern. Wenn Sie damit fertig sind, klicken Sie **`Aktualisiere Konfig`**.

1.3. Mehrfache Satellites

Inter-Satellite Synchronization (ISS) ermöglicht es einem Satellite, Inhalte und Berechtigungen mit einer anderen Satellite Instanz in einer *peer-to-peer* Beziehung zu synchronisieren. Jedoch wird im folgenden Abschnitt ein Satellite, der Inhalte empfängt, als "Slave Satellite" und ein Satellite, der als Quelle dient, von wo der Inhalt gezogen wird, als "Master Satellite" bezeichnet werden. Bei der Verwendung von ISS den Inhalt zu synchronisieren, kann die Slave Satellite Instanz eine andere Einstellung als der Master haben für Nicht-Inhalt Entitäten wie Benutzer und Organisationen. Der Satellite Administrator auf der Slave-Instanz kann Entitäten frei hinzufügen, entfernen und ändern, unabhängig von dem was auf der Master-Instanz geschieht.

Anmerkung

Master und Slave sind vererbte Begriffe, die Nebenbedeutungen tragen, die vom ISS-Protokoll *nicht erzwungen* werden. Bitte beachten Sie die eingeschränkten Bedeutungen, wie oben beschrieben, während dem Studium dieses Abschnitts.

Die ISS-Funktion kann auf verschiedene Weise, je nach den Bedürfnissen der Organisation, verwendet werden. Es gibt ISS Konfigurationen, bei denen zwei Satellites als jeweilige Master und Slaves voneinander agieren können. Dieser Abschnitt enthält einen Abschnitt über Anwendungsfälle und wie ISS am besten eingerichtet und Ihrer Organisation angepasst werden kann.

ISS-Voraussetzungen

Folgende Bedingungen müssen für den Einsatz von ISS erfüllt sein:

- Zwei oder mehr Red Hat Satellite Server
- Mindestens ein Red Hat Satellite, der mit mindestens einem Channel bestückt ist
- Satellite Administrator-Rechte auf allen Satellite Systemen, die für ISS bestimmt sind

1.3.1. Inter-Satellite-Synchronisation

ISS kann manuell oder durch ein neues Tool namens **`spacewalk-sync-setup`** konfiguriert werden. Beide Methoden sind effektiv, und es bleibt der Wahl des Benutzers überlassen, welche verwendet wird.

1.3.1.1. Manuelle Konfiguration

Prozedur 1.1. Konfiguration des Master Saltellite Servers

Mit Satellite 5.6 ermöglicht ISS dem Slave Satellite, die organisatorische Vertrauens-Hierarchie und die benutzerdefinierten Channel Berechtigungen von den konfigurierten Einstellungen auf dem Master zu duplizieren. Dies wird durch den Export von Informationen über bestimmte Organisationen vom Master Satellite an den empfangenden Slave Satellite erreicht. Der Satellite Administrator auf dem Slave Satellite kann dann entscheiden, die Master Organisationen auf bestimmte Slave Organisationen abzubilden. Zukünftige **`satellite-sync`** Operationen benutzen diese Informationen, um benutzerdefiniertes Channel-Eigentum derjenigen Slave Organisation zuzuweisen, die zu einer bestimmten Master Organisation zugeordnet ist. Es kann auch die Vertrauensbeziehungen zwischen der exponierten Master Organisation auf passende Slave Organisationen abbilden und erstellt daher die gleichwertigen Beziehungen auf dem Slave.

1. Auf der Weboberfläche:
    a. Melden Sie sich als der Satellite-Administrator an.
    b. Klicken Sie **Admin** → **ISS Configuration** → **Master Setup**.

c. Klicken Sie in der rechten oberen Ecke **Add New Slave**.

d. Füllen Sie die folgende Information aus:

- Slave Fully Qualified Domain Name (FQDN)
- Ermöglichen Slave zu synchronisieren? - Die Auswahl dieses Feldes ermöglicht dem Slave Satellite auf diesen Master Satellite zugreifen. Andernfalls wird Kontakt mit diesem Slave verweigert werden.
- Synchronisieren alle Organisationen zum Slave? - Aktivieren dieses Feldes wird alle Organisationen zum Slave Satellite synchronisieren.

Anmerkung

Auswahl der **Sync All Orgs to Slave?** Option auf der Master-Setup-Seite überschreibt alle speziell ausgewählten Organisationen in der lokalen Organisations-Tabelle unten.

e. Klicken Sie **Create**.

f. (Optional) Klicken Sie auf jede lokale Organisation, die auf den Slave Satellite exportiert werden soll.

g. Klicken Sie **Allow Orgs**.

Anmerkung

In Satellite 5.5 verwendete der Master Satellite den ***iss_slaves*** Parameter in der **/etc/rhn/rhn.conf** Datei um zu identifizieren, welche Sklaven den Meister Satellite kontaktieren konnten. Satellite 5.6 verwendet die Information in der Master-Setup Seite, um diese Information zu ermitteln.

2. Auf der Befehlszeile

a. Aktivieren Sie das Inter-Satellite Synchronisation (ISS) Feature in der **/etc/rhn/rhn.conf** Datei:

```
disable_iss=0
```

b. Speichern Sie die Konfigurationsdatei ab und starten den **httpd**-Dienst neu:

```
service httpd restart
```

Prozedur 1.2. Konfiguration der Slave-Server

Slave-Satellite-Server sind diejenigen Rechner, die synchronisierte Inhalte vom Master Server erhalten werden.

1. Um Inhalte sicher auf die Slave-Server zu übertragen, benötigen Sie das **ORG-SSL** Zertifikat von Ihrem Master-Server. Sie können das Zertifikat über HTTP vom **/pub/** Verzeichnis eines beliebigen Satellite heruntergeladen. Die Datei heißt **RHN-ORG-TRUSTED-SSL-CERT**, kann jedoch umbenannt und an einem beliebigen Speicherort auf dem Slave-Satellite abgelegt werden, wie z.B. im **/usr/share/rhn/** Verzeichnis.
2. Melden Sie sich auf dem Slave Saltellite als der Satellite-Administrator an.
3. Klicken Sie **Admin** → **ISS Configuration** → **Slave Setup**.

4. Klicken Sie in der rechten oberen Ecke **`Add New Master`**.
5. Füllen Sie die folgende Information aus:
   - Master Fully Qualified Domain Name
   - Standard Master?
   - Dateiname des CA-Zertifikats dieses Masters - Verwenden Sie den vollständigen Pfad des CA-Zertifikats, das im ersten Schritt dieses Verfahrens heruntergeladen wurde.
6. Klicken Sie **`Add New Master`**.

Prozedur 1.3. Durchführen einer Inter-Satellite-Synchronisation

Nachdem die Master- und Slave-Server konfiguriert wurden, können Sie nun eine Synchronisation zwischen den beiden durchführen.

- Beginnen Sie die Synchronisation durch Ausführen des Befehls **`satellite-sync`**:

```
satellite-sync -c your-channel
```

Anmerkung

Befehlszeilenoptionen, die Sie beim **`satellite-sync`** Befehl manuell angeben, setzen die benutzerdefinierten Einstellungen in der **`/etc/rhn/rhn.conf`** Datei außer Kraft.

Prozedur 1.4. Abbildung der Exportierten Organisationen des Master Satellite an die Organisationen des Slave Satellite

Vorbedingung

Nach Durchführung der vorherigen Verfahren sollte der Master Satellite sich im Slave Satellite Slave Setup unter **Admin → ISS Configuration → Slave Setup** zeigen. Wenn nicht, überprüfen Sie bitte nochmals die oben genannten Schritte.

Eine Zuordnung zwischen organisatorischen Namen auf dem Master Satellite erlaubt dass Channel Zugriffs-Berechtigungen auf dem Master Satellite erstellt und weitergegeben werden, wenn der Inhalt mit einem Slave Satellite synchronisiert wird. Nicht alle Organisations- und Channel-Details müssen für alle Slave Satellites zugeordnet werden, Satellite Administratoren können auswählen, welche Berechtigungen und Organisationen synchronisiert werden können, indem sie Zuordnungen erlauben oder weglassen.

Um die Zuordnung zu vervollständigen, folgen Sie diesem Verfahren auf dem Slave Satellite:

1. Melden Sie sich als der Satellite-Administrator an.
2. Klicken Sie **Admin → ISS Configuration → Slave Setup**.
3. Wählen Sie einen Master Satellite indem Sie auf seinen Namen klicken.
4. Verwenden Sie die Auswahl-Liste, um den exportierten Master Organisations-Namen zu einer passenden lokalen Organisation im Slave Satellite zuzuordnen.
5. Klicken Sie **`Update Mapping`**.
6. In der Befehlszeile geben Sie den **`satellite-sync`** auf jedem der benutzerdefinierten Channels ein, um die richtige Vertrauens-Struktur und richtigen Channel-Berechtigungen zu erhalten:

```
satellite-sync -c your-channel
```

1.3.1.2. Automatisierte Konfiguration

spacewalk-sync-setup ermöglicht es Benutzern, eine Master und Slave Satellite Instanz anzugeben und verwendet Konfigurationsdateien, um die Informationen, die sowohl im Master und Slave Setup beschrieben sind, zu installieren. Es kann, falls gewünscht, eine Reihe von Standard-Konfigurationsdateien erstellen. Im Wesentlichen automatisiert es die zuvor vorbereitete und zugeordnete Konfiguration für Master-Slave-Beziehungen.

Voraussetzungen

Damit die automatische Konfiguration erfolgreich ist:

- Das *spacewalk-util* Paket muss auf dem System, das den Befehl **spacewalk-sync-setup** ausgeben wird, installiert sein.
- Bestehende Organisationen mit benutzerdefinierten Berechtigungen auf dem Master Satellite müssen vorhanden sein.
- Bestehende Organisationen innerhalb des Slave Satellite müssen vorhanden sein.

Prozedur 1.5. Konfiguration des Master Saltellite Servers

1. Aktivieren Sie das Inter-Satellite Synchronisation (ISS) Feature in der **/etc/rhn/rhn.conf** Datei:

```
disable_iss=0
```

2. Speichern Sie die Konfigurationsdatei ab und starten den **httpd**-Dienst neu:

```
service httpd restart
```

Prozedur 1.6. Konfiguration der Slave-Server

Slave-Satellite-Server sind diejenigen Rechner, deren Inhalte mit dem Master-Server synchronisiert werden.

1. Um Inhalte sicher auf die Slave-Server zu übertragen, benötigen Sie das **ORG-SSL** Zertifikat von Ihrem Master-Server. Sie können das Zertifikat über HTTP vom **/pub/** Verzeichnis eines beliebigen Satellite heruntergeladen. Die Datei heißt **RHN-ORG-TRUSTED-SSL-CERT**, kann jedoch umbenannt und an einem beliebigen Speicherort auf dem Slave-Satellite abgelegt werden, wie z.B. im **/usr/share/rhn/** Verzeichnis.
2. Melden Sie sich auf dem Slave Saltellite als der Satellite-Administrator an.
3. Klicken Sie **Admin** → **ISS Configuration** → **Slave Setup**.
4. Klicken Sie in der rechten oberen Ecke **Add New Master**.
5. Füllen Sie die folgende Information aus:
   - Master Fully Qualified Domain Name
   - Standard Master?
   - Dateiname des CA-Zertifikats dieses Masters - Verwenden Sie den vollständigen Pfad des CA-Zertifikats, das im ersten Schritt dieses Verfahrens heruntergeladen wurde.
6. Klicken Sie **Add New Master**.

Prozedur 1.7. Abbildung der Organisationen des Master Satellite auf die Organisationen des Slave Satellite mit spacewalk-sync-setup

1. Melden Sie sich in einem System an. Es spielt keine Rolle, ob es ein Master Satellite, ein Slave

Satellite oder ein insgesamt anderes System ist, solange das System auf das öffentliche XMLRPC API der Master und Slave Satellites zugreifen kann.

2. Geben Sie **`spacewalk-sync-setup`** auf einer Befehlszeilenschnittstelle ein:

```
spacewalk-sync-setup --ms=[Master_FQDN] \
--ml=[Master_Sat_Admin_login] \
--mp=[Master_Sat_Admin_password] \
--ss=[Slave FQDN]  --sl=[Slave_Sat_Admin_login] \
--sp=[Slave_Sat_Admin_password> \
--create-templates --apply
```

Wobei gilt:

- --ms=MASTER, --master-server=MASTER ist der FQDN des Masters der Verbindung
- --ml=MASTER_LOGIN, --master-login=MASTER_LOGIN ist das Login des Satellite Administrator für den Master Satellite
- --mp=MASTER_PASSWORD, --master-password=MASTER_PASSWORD ist das Passwort für das Login des Satellite Administrator auf dem Master Satellite
- --ss=SLAVE, --slave-server=SLAVE ist der FQDN des Slave Satellite der Verbindung.
- --sl=SLAVE_LOGIN, --slave-login=SLAVE_LOGIN ist das Login des Satellite Administrator für den Slave Satellite
- --sp=SLAVE_PASSWORD, --slave-password=SLAVE_PASSWORD ist das Passwort für das Login des Satellite Administrator auf dem Slave Satellite
- --ct, --create-templates ist die Option, die sowohl eine Master und eine Slave Setup-Datei für das Master/Slave-Paar, auf das wir gezeigt haben, erstellt
- --apply zeigt den Satellite-Instanzen an, die Änderungen, die durch die Setup-Dateien angegeben werden, an den angegebenen Satellite Instanzen durchzuführen

Anmerkung

Für weitere Setup-Optionen:

```
spacewalk-sync-setup --help
```

Die Ausgabe von diesem Befehl ist wie folgt:

```
INFO: Connecting to [admin@master-fqdn]
INFO: Connecting to [admin@slave-fqdn]
INFO: Generating master-setup file $HOME/.spacewalk-sync-setup/master.txt
INFO: Generating slave-setup file $HOME/.spacewalk-sync-setup/slave.txt
INFO: Applying master-setup $HOME/.spacewalk-sync-setup/master.txt
INFO: Applying slave-setup $HOME/.spacewalk-sync-setup/slave.txt
```

3. In der Befehlszeile geben Sie den **`satellite-sync`** Befehl auf jedem der benutzerdefinierten Channels ein, um die richtige Vertrauens-Struktur und richtigen Channel-Berechtigungen zu erhalten:

```
satellite-sync -c your-channel
```

1.3.2. Organisationssynchronisation

Inter-Satellite Synchronization kann auch dazu verwendet werden, um Inhalte in eine bestimmte

Organisation zu importieren. Dies kann entweder lokal oder durch externe Synchronisation erfolgen. Diese Funktion ist hilfreich für einen nicht verbundenen Satellite mit mehreren Organisationen, wo Inhalte über Channel-Dumps oder durch Export von verbundenen Satellites und anschließenden Import zum nicht verbundenen Satellite bezogen werden. Organisations-Synchronisation kann verwendet werden, um spezifische Channels von verbundenen Satellites zu exportieren. Es kann auch effektiv dazu genutzt werden, um Inhalte zwischen Organisationen zu verschieben.

Organisations-Synchronisation folgt einer Reihe von klaren Regeln, um die Integrität der Quellorganisation zu wahren.

- Falls die Quellinhalte zur ***NULL*** Organisation gehören (also jegliche Red Hat Inhalte), wird standardmäßig die ***NULL*** Organisation gewählt, selbst wenn eine Zielorganisation angegeben wurde. Dies gewährleistet, dass sich der angegebene Inhalt immer in der privilegierten ***NULL*** Organisation befindet.
- Wird auf der Befehlszeile eine Organisation angegeben, werden Inhalte von dieser Organisation importiert.
- Wird keine Organisation angegeben, wird standardmäßig Organisation 1 gewählt.

Im Folgenden sehen Sie drei Beispielszenarien, in denen Organisations-IDs (***orgid***) zur Synchronisation zwischen Satellites verwendet werden:

Beispiel 1.1. Inhalte vom Master zum Slave Satellite importieren

In diesem Beispiel werden Inhalte vom Master zum Slave Satellite importiert:

```
satellite-sync --parent-sat=master.satellite.example.com -c channel-name --
orgid=2
```

Beispiel 1.2. Inhalte von einem exportierten Dump einer Organisation importieren

In diesem Beispiel werden Inhalte von einem exportierten Dump einer bestimmten Organisation importiert:

```
$ satellite-sync -m /dump -c channel-name --orgid=2
```

Beispiel 1.3. Importieren von Inhalten von Red Hat Network Hosted

In diesem Beispiel werden Inhalte von Red Hat Network Hosted importiert (vorausgesetzt, das System ist registriert und aktiviert):

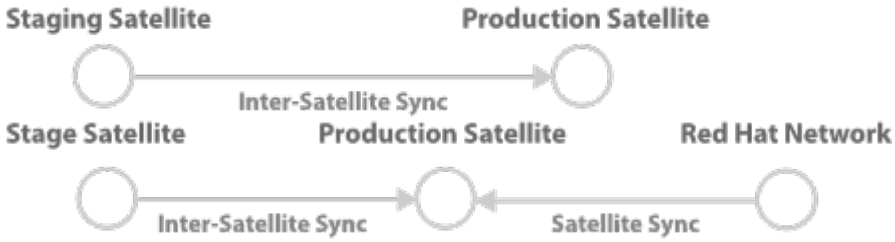
```
$ satellite-sync -c channel-name
```

1.3.3. Inter-Satellite Synchronisation Anwendungsfälle

Inter-Satellite Synchronization (ISS) kann auf verschiedene Arten eingesetzt werden, abhängig von den Anforderungen Ihrer Organisation. Dieser Abschnitt liefert Beispiele für mögliche Anwendungsfälle von ISS sowie die Methoden zum Einrichten und Durchführen dieser Fälle.

Beispiel 1.4. Staging-Satellite

In diesem Beispiel wird ein Satellite als *Staging-Satellite* zur Vorbereitung von Inhalten und zur Durchführung von Aufgaben zur Qualitätssicherung eingesetzt, um sicherzustellen, dass Pakete für den Einsatz in einer Produktionsumgebung bereit sind. Nachdem Inhalte für die Produktion freigegeben wurden, kann der Produktions-Satellite die Inhalte vom Staging-Satellite synchronisieren.



1. Führen Sie den **`satellite-sync`** Befehl aus, um Daten mit dem **`rhn_parent`** (in der Regel Red Hat Network Hosted) zu synchronisieren:

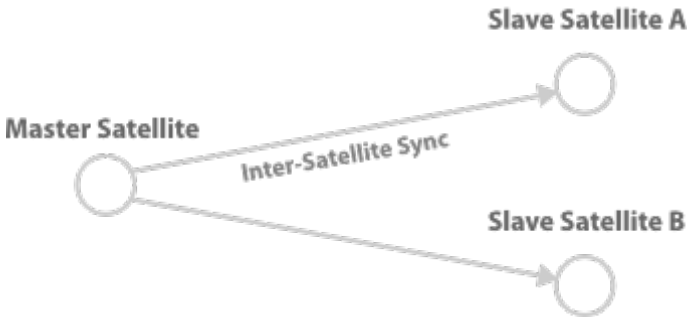
```
satellite-sync -c your-channel
```

2. Führen Sie folgenden Befehl aus, um Daten vom Staging-Server zu synchronisieren:

```
satellite-sync --iss-parent=staging-satellite.example.com -c custom-channel
```

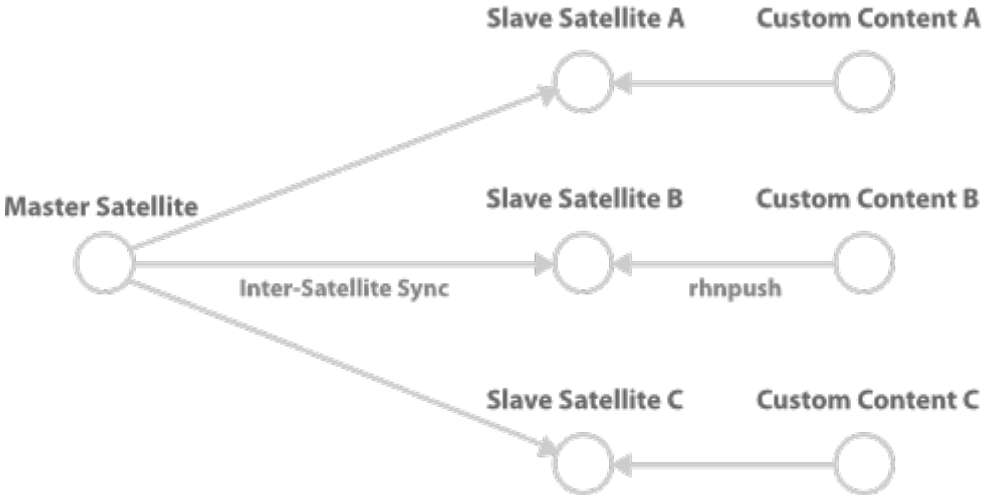
Beispiel 1.5. Synchronisierte Slaves

In diesem Beispiel liefert der Master Satellite Daten direkt an seine Slaves und Änderungen werden regelmäßig synchronisiert.



Beispiel 1.6. Benutzerdefinierte Inhalte auf den Slaves

In diesem Beispiel wird der Master Satellite als Entwicklungs-Channel genutzt, von dem Inhalte auf alle Produktions Slave Satellites synchronisiert werden. Einige der Slave Satellites verfügen über zusätzliche Inhalte, die nicht auf den Channels des Master Satellites vorliegen. Diese Pakete werden bewahrt, alle anderen Änderungen vom Master Satellite jedoch werden auf den Slaves synchronisiert.



Beispiel 1.7. Bi-direktionale Synchronisation

In diesem Umfeld agieren zwei Red Hat Satellite Server als Master und Slave zueinander und können Inhalte zwischen ihnen zu synchronisieren. Der Satellite Server, auf dem der Befehl **`satellite-sync`** durchgeführt wird, zieht den Inhalt vom anderen Satellite Server ab und die synchronisierten Daten werden von den Optionen, mit denen **`satellite-sync`** ausgeführt wird, abhängen. Ohne Optionen wird die Synchronisierung versuchen alles zu aktualisieren, was zuvor synchronisiert wurde.

Siehe Abschnitt 1.3.1.1, „Manuelle Konfiguration“ für die Konfiguration eines Master-Satellite. Konfiguration beider Satellite Server als Master wird eine bi-direktionale Synchronisation erstellen.

Kapitel 2. Red Hat Satellite und Solaris-spezifische Information

Dies ist ein Abschnitt über die Verwendung von Red Hat Satellite mit Solaris Systemen.

2.1. UNIX Unterstützungs-Handbuch

2.1.1. Einführung

Dieses Kapitel behandelt den Installationsvorgang und beschreibt die Unterschiede in Red Hat Network Funktionalität bei der Verwaltung UNIX-basierter Client-Systeme. Red Hat Network bietet UNIX-Unterstützung, um Kunden bei der Migration von UNIX zu Linux zu helfen. Die Features, die zur Verwaltung von UNIX-Clients angeboten werden, sind nicht so umfassend wie die Features, die zur Verwaltung von Red Hat Enterprise Linux Systemen zur Verfügung stehen.

Die nachfolgenden Abschnitte behandeln unterstützte UNIX-Varianten, Red Hat Network Features, die vom UNIX-Management-System unterstützt werden, die Voraussetzungen, um ein UNIX-System mit Red Hat Network verwalten zu können sowie den Installationsvorgang für UNIX-Clients.

2.1.1.1. Unterstützte UNIX-Varianten

Die folgenden UNIX-Varianten, Versionen und Architekturen werden von Red Hat Network Satellite unterstützt:

Tabelle 2.1. Unterstützte Solaris Architekturen und Versionen

Solaris Version	sun4m	sun4d	sun4u	sun4v	sun4us	x86
Solaris 8	ja	nein	ja	k.A.	nein	nein
Solaris 9	ja	k.A.	ja	k.A.	nein	ja
Solaris 10	k.A.	k.A.	ja	ja	nein	ja

2.1.1.2. Voraussetzungen

Dies wird zur UNIX-Unterstützung benötigt:

- Red Hat Satellite 5.0 oder höher
- Ein Satellite-Zertifikat mit Management-Berechtigungen
- Management-Berechtigungen für jeden UNIX-Client
- Red Hat Network Pakete für UNIX, inklusive Python, pyOpenSSL und die Red Hat Network Client Pakete
- Sunfreeware-Pakete, die unterstützende Bibliotheken bereitstellen.

Anmerkung

Einige dieser Pakete sind via Red Hat Satellite verfügbar. Siehe Abschnitt 2.1.3.1, „Herunterladen und Installation zusätzlicher Pakete“ für eine vollständige Liste.

2.1.1.3. Enthaltene Features

Die folgenden Features sind in der UNIX Unterstützung Service-Level Vereinbarung enthalten da sie innerhalb von Red Hat Network existieren:

- Der **Red Hat Network Service Daemon** (**rhnsd**), welcher **rhn_check** gemäß eines konfigurierbaren Intervalls auslöst
- Der **Red Hat Network Configuration Client** (**rhncfg-client**), welcher sämtliche vom Satellite eingeplante Konfigurationsaktionen ausführt
- Der **Red Hat Network Configuration Manager** (**rhncfg-manager**), welcher die Befehlszeilenverwaltung von Red Hat Network Konfigurations-Channels ermöglicht
- Das **rhn_check** Programm, welches sich beim Satellite anmeldet und alle vom Server aus geplanten Aktionen durchführt
- Jegliche Funktionalität auf Management-Ebene, wie beispielsweise System-Gruppierung, Paket-Profil-Vergleich und die Verwendung des System-Set-Managers, um mehrere Systeme gleichzeitig zu betreuen
- Das Provisioning-Feature *Remote Command*, welches Benutzern ermöglicht, Befehle auf Root-Ebene auf jedem verwalteten Client mittels der Website des Satellite einzuplanen, sofern der Client dies zulässt

2.1.1.4. Unterschiede in der Funktionalität

Die folgenden Red Hat Network Features funktionieren in einer UNIX-Umgebung anders:

- Der **Red Hat Update Agent für UNIX** bietet weitaus weniger Optionen als dessen Linux-Gegenstück und arbeitet mit dem systemeigenen Betriebssystem-Toolset für Paket-Installation anstatt mit **rpm** - Siehe Abschnitt 2.1.4.2.4, „Von der Befehlszeile aus aktualisieren“ für eine umfassende Liste der Optionen.
- Die **Red Hat Network Push** Applikation wurde auf ähnliche Weise modifiziert, um systemeigene UNIX-Dateitypen hochzuladen, wie u.a. Pakete, Patches und Patch-Cluster.

  Da sich Solaris Paket-, Patch- und Patch-Cluster-Dateien von rpm-Dateien unterscheiden, ist auch der Channel-Upload-Mechanismus etwas anders. Es gibt zwei Applikationen im **rhnpush** Paket für Solaris:
  - Der erste Befehl, **solaris2mpm**, ist ein Red Hat Network Dienstprogramm, das eine MPM-Datei für jedes Solaris-Paket oder jeden Solaris-Patch erstellt. Das neutrale Format der MPM-Datei erlaubt es dem Satellite, hochgeladene Dateien zu verstehen und zu verwalten.
  - Der zweite Befehl, **rhnpush**, wurde erweitert damit er sowohl MPM- als auch RPM-Dateien verarbeiten kann. Ansonsten funktioniert er identisch zur Linux-Version von **rhnpush**.
- Der **Channels** Tab der Red Hat Network Website wurde erweitert um die Speicherung und Installation systemeigener UNIX-Dateitypen zuzulassen.

2.1.1.5. Ausgeschlossene Features

Die folgenden Red Hat Network Features sind nicht mit dem UNIX-Support-System verfügbar:

- Funktionalität auf Provisioning-Stufe, wie beispielsweise Kickstart und Paket-Rollback, mit der Ausnahme von Konfigurations-Datei Management
- Alle Errata-bezogenen Optionen, da es das Konzept von Errata-Updates in UNIX nicht gibt
- Quelldateien für Pakete

Answer Dateien werden noch nicht unterstützt. Die Unterstützung für diese Art von Dateien ist jedoch für ein zukünftiges Release geplant.

IPv6 wird auf Solaris-Systemen ebenfalls nicht unterstützt.

Zudem wird das Verlagern der **RHAT*.pkg** Dateien an einen anderen Ort während der Installation nicht unterstützt.

2.1.2. Satellite Server Vorbereitung/Konfiguration

Sie müssen den Satellite konfigurieren die UNIX-Clients zu unterstützen bevor die benötigten Dateien zur Implementierung auf den Client-Systemen zur Verfügung stehen. Dies kann auf zwei Arten geschehen und hängt davon ab, ob Sie Ihren Satellite Server bereits installiert haben:

1. Während der Satellite-Installation:

   Aktivieren Sie die UNIX-Unterstützung auf dem Satellite, indem Sie das "Enable Solaris Support (Solaris Support aktivieren)" Kästchen während des Installationsprozesses, wie hier abgebildet, auswählen:

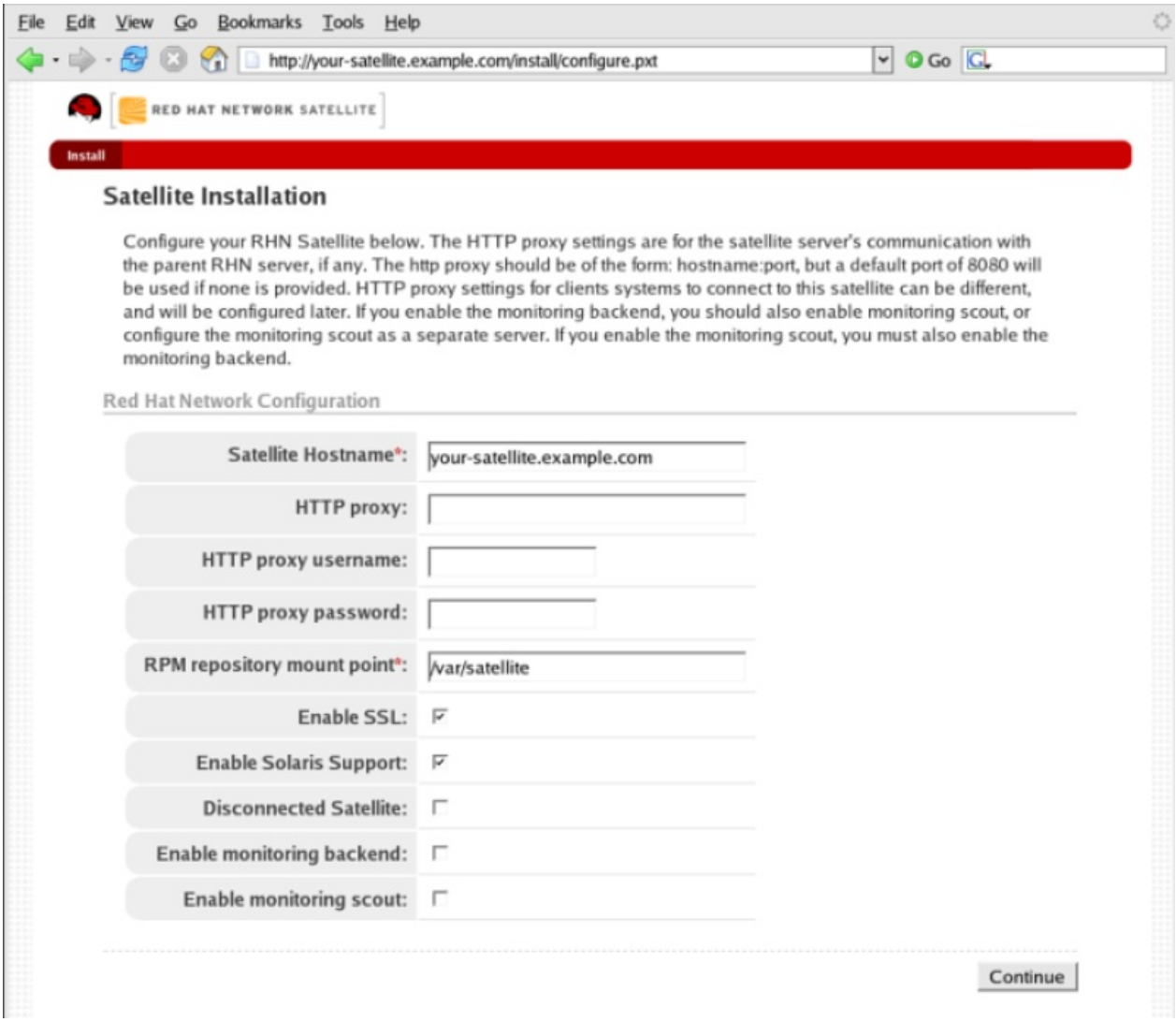

File Edit View Go Bookmarks Tools Help
http://your-satellite.example.com/install/configure.pxt
Go
RED HAT NETWORK SATELLITE
Install
Satellite Installation
Configure your RHN Satellite below. The HTTP proxy settings are for the satellite server's communication with the parent RHN server, if any. The http proxy should be of the form: hostname:port, but a default port of 8080 will be used if none is provided. HTTP proxy settings for clients systems to connect to this satellite can be different, and will be configured later. If you enable the monitoring backend, you should also enable monitoring scout, or configure the monitoring scout as a separate server. If you enable the monitoring scout, you must also enable the monitoring backend.
Red Hat Network Configuration
Satellite Hostname*:
your-satellite.example.com
HTTP proxy:
HTTP proxy username:
HTTP proxy password:
RPM repository mount point*:
/var/satellite
Enable SSL:
Enable Solaris Support:
Disconnected Satellite:
Enable monitoring backend:
Enable monitoring scout:
Continue

Abbildung 2.1. UNIX-Unterstützung während der Satellite-Installation aktivieren

2. Nachdem der Satellite installiert wurde:

   Aktivieren Sie die UNIX-Unterstützung, indem Sie den Satellite nach dessen Installation konfigurieren. Dazu wählen Sie **Admin** in der oberen Menüleiste aus und dann **Satellite-Konfiguration** in der linken Navigationsleiste. Auf dem folgenden Bildschirm klicken Sie das **`Enable Solaris Support`** Kästchen (siehe Abbildung):

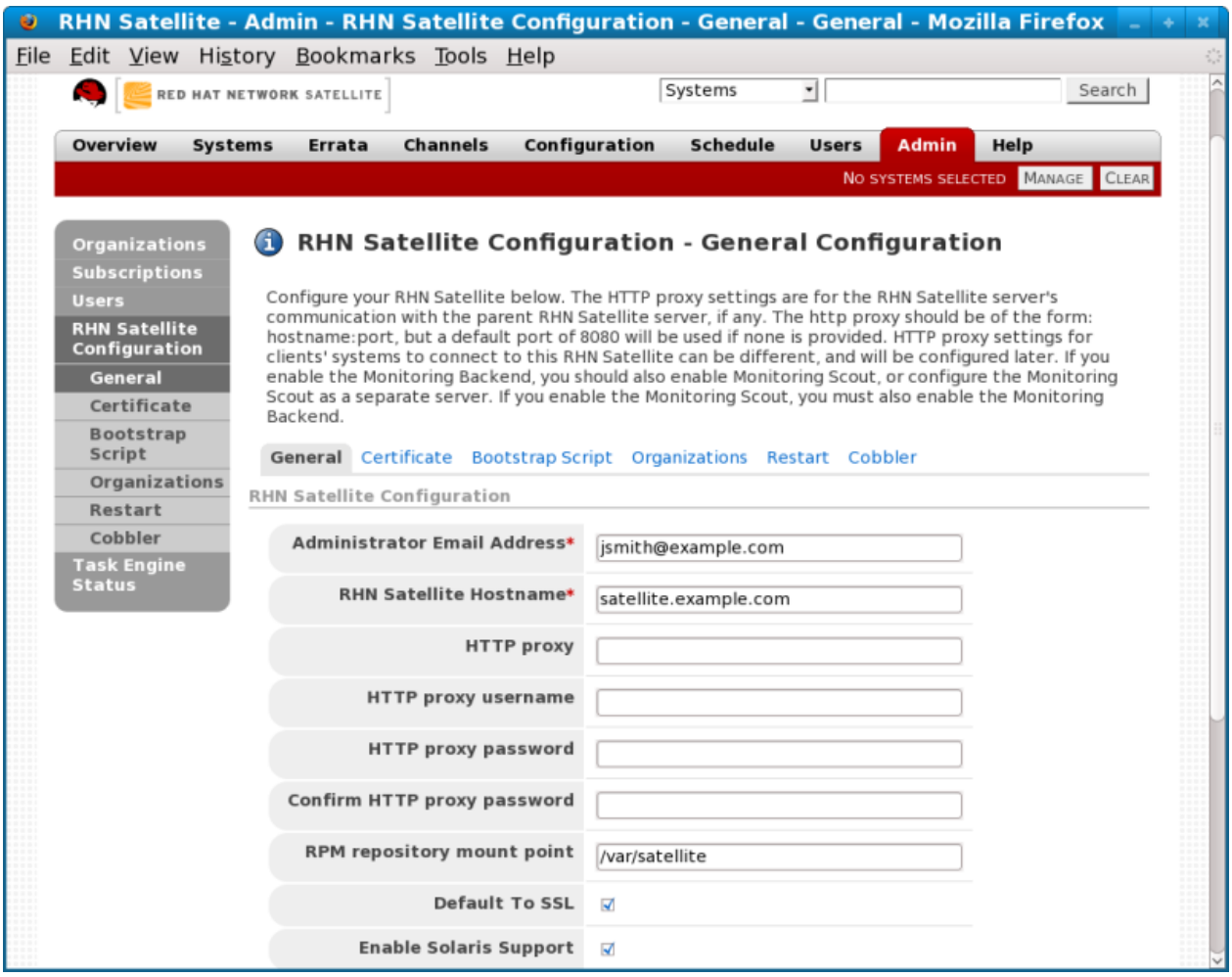

RHN Satellite - Admin - RHN Satellite Configuration - General - General - Mozilla Firefox
File Edit View History Bookmarks Tools Help
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Admin Help
No systems selected Manage Clear
Organizations
Subscriptions
Users
RHN Satellite Configuration
General
Certificate
Bootstrap Script
Organizations
Restart
Cobbler
Task Engine Status
RHN Satellite Configuration - General Configuration
Configure your RHN Satellite below. The HTTP proxy settings are for the RHN Satellite server's communication with the parent RHN Satellite server, if any. The http proxy should be of the form: hostname:port, but a default port of 8080 will be used if none is provided. HTTP proxy settings for clients' systems to connect to this RHN Satellite can be different, and will be configured later. If you enable the Monitoring Backend, you should also enable Monitoring Scout, or configure the Monitoring Scout as a separate server. If you enable the Monitoring Scout, you must also enable the Monitoring Backend.
General Certificate Bootstrap Script Organizations Restart Cobbler
RHN Satellite Configuration
Administrator Email Address* jsmith@example.com
RHN Satellite Hostname* satellite.example.com
HTTP proxy
HTTP proxy username
HTTP proxy password
Confirm HTTP proxy password
RPM repository mount point /var/satellite
Default To SSL
Enable Solaris Support

Abbildung 2.2. UNIX-Unterstützung nach der Satellite-Installation aktivieren

Klicken Sie auf die Schaltfläche **`Konfiguration aktualisieren`**, um die Änderung zu bestätigen.

3. Erstellen Sie abschließend einen Basis-Channel, den Ihr Client subskribieren kann. Dieser Schritt ist nötig, da Red Hat Network keinen UNIX-Inhalt liefert. Somit können Sie nicht **`satellite-sync`** zur Erstellung eines Channels verwenden.

   Um einen Solaris-Channel zu erstellen, melden Sie sich auf der Weboberfläche des Satellites entweder als Satellite-Administrator oder als Zertifizierungsstelle ein. Gehen Sie auf den **`Channel`** Tab, gefolgt von **`Software-Channels verwalten`** in der linken Navigationsleiste. Klicken Sie auf den Link **`Neuen Channel erstellen`** im rechten oberen Bereich des daraufhin angezeigten Bildschirms. Geben Sie einen Namen und ein Label für Ihren neuen Channel ein und wählen Sie entweder **`Sparc Solaris`** oder **`i386 Solaris`** als Architektur aus, abhängig von der Architektur Ihres Clients.

2.1.3. Vorbereitung des Unix-Client-Systems

Bevor Ihre UNIX-basierten Client-Systeme von Red Hat Network profitieren können, müssen sie für die Verbindung eingerichtet werden:

1. Laden Sie **`gzip`** und die erforderlichen Bibliotheken von Drittanbietern herunter und installieren diese.
2. Laden Sie den Red Hat Network Applikations-Tarball vom Satellite auf den Client herunter und installieren den Inhalt.

3. Implementieren Sie als Nächstes die für eine sichere Verbindung benötigten SSL-Zertifikate.
4. Konfigurieren Sie die Client-Applikationen zur Verbindung mit dem Red Hat Satellite.

Nach Abschluss ist Ihr System bereit, mit dem Empfang von Red Hat Network-Updates zu beginnen. Die folgenden Abschnitte erklären diese Schritte im Detail.

2.1.3.1. Herunterladen und Installation zusätzlicher Pakete

Dieser Abschnitt führt Sie durch den Vorgang zum Herunterladen und Installieren der Anwendungen von Drittanbietern und der Red Hat Network-Anwendungen vom Satellite auf den UNIX-Client.

Von zentraler Bedeutung ist der **Red Hat Update Agent für UNIX** (**`up2date`**), der die Verbindung zwischen Ihren Client-Systemen und Red Hat Network darstellt. Die UNIX-spezifische Version des **Red Hat Update Agent** ist im Vergleich zu seinem Linux-Gegenstücken in seiner Funktionalität eingeschränkt, ermöglicht jedoch immer noch die Systemregistrierung und erleichtert die Installation von Paketen und Patches. Siehe Abschnitt 2.1.4, „Registrierung und Updates für Unix-Clients“ für eine umfassende Beschreibung der Optionen des Tools.

Anmerkung

Es ist möglicherweise hilfreich, den Befehl **`bash`** beim ersten Anmelden auf dem Solaris-Client auszuführen. Falls die BASH-Shell zur Verfügung steht, verhält sich das System so ähnlich wie Linux wie möglich.

2.1.3.1.1. Pakete von Drittanbietern installieren

Die Installation der Red Hat Network-Anwendungen kann nicht fortgesetzt werden, bis folgende Dienstprogramme und Bibliotheken vorhanden sind:

- **`gzip`**
- **`libgcc`**
- **`openssl`**
- **`zlib`**

Das Dienstprogramm **`gzip`** wird vom SUNW Paket 'gzip' geliefert und kann von http://www.sunfreeware.com heruntergeladen werden.

Auf kürzlich installierten Solaris-Versionen werden die notwendigen Bibliotheken von den folgenden standardmäßig installierten Paketen geliefert:

- **`SUNWgccruntime`**
- **`SUNWopenssl*`**
- **`SUNWzlib`**

Für ältere Solaris-Versionen können die folgenden benötigten Pakete von http://www.sunfreeware.com heruntergeladen werden:

- **`SMClibgcc`** oder **`SMCgcc`**
- **`SMCossl`**
- **`SMCzlib`**

Verwenden Sie den Befehl **`pkginfo`**, um zu überprüfen, ob ein Paket auf dem Client installiert ist. Um beispielsweise nach einem Paket zu suchen, das "zlib" im Namen enthält, führen Sie den folgenden

Befehl aus:

```
# pkginfo | grep zlib
```

Anmerkung

Solaris-Paketarchivnamen unterscheiden sich vom Namen des installierten Pakets. So wird das Paketarchiv **libgcc<version>-sol<solaris-version>-sparc-local.gz** nach der Installation zu SMClibgcc.

2.1.3.1.2. Suchpfad der Bibliothek konfigurieren

Um dem Solaris-Client die Verwendung der im vorherigen Schritt installierten Bibliotheken zu gestatten, müssen Sie deren Speicherort zum Bibliotheks-Suchpfad hinzufügen. Überprüfen Sie diesbezüglich zunächst den derzeitigen Bibliotheks-Suchpfad:

```
# crle -c /var/ld/ld.config
```

Notieren Sie sich den aktuellen Standard-Bibliothekspfad. Passen Sie als Nächstes den Pfad so an, dass er die unten aufgeführten Komponenten umfasst. Beachten Sie, dass die Option **-l** den Wert zurücksetzt, anstatt ihn anzuhängen. Falls daher bereits Werte auf Ihrem System eingerichtet waren, stellen Sie diese dem -l-Parameter voran.

Auf SPARC:

```
 # crle -c /var/ld/ld.config -l /other/existing/path:/lib:/usr/lib:/usr/local/lib
```

Auf x86:

```
# crle -c /var/ld/ld.config -l
/other/existing/path:/lib:/usr/lib:/usr/local/lib:/usr/sfw/lib
```

2.1.3.1.3. Red Hat Network-Client-Pakete herunterladen

Laden Sie den entsprechenden Tarball von Paketen aus dem Verzeichnis **/var/www/html/pub/** Ihres Satellites herunter. Falls Sie keinen GUI-Webbrowser wie Mozilla verwenden können, navigieren Sie zum Verzeichnis **/pub** des Satellite und speichern den entsprechenden Tarball auf Ihrem Client:

```
http://your-satellite.example.com/pub/rhn-solaris-bootstrap-<version>-<solaris-
arch>-<solaris-version>.tar.gz
```

Falls Sie den Tarball von der Kommandozeile aus herunterladen müssen, sollte es möglich sein, die Datei mithilfe von **ftp** vom Satellite auf den Client zu übertragen.

Entpacken Sie den Tarball unter Verwendung von **gzip**. Sie sollten jetzt die folgenden Pakete besitzen:

- **RHATpossl**
- **RHATrhnrcfg**
- **RHATrhnrcfga**
- **RHATrhnrcfgc**
- **RHATrhnrcfgm**

- **RHATrhnc**
- **RHATrhnl**
- **RHATrpush**
- **RHATsmart**

SMClibgcc und **SMCosslg** können ebenfalls im Tarball enthalten sein.

2.1.3.1.4. Installieren der Red Hat Netzwerk-Pakete

Wechseln Sie in das entpackte Verzeichnis und verwenden Sie die Standard-Installationstools der UNIX-Variante, um jedes Paket zu installieren. Verwenden Sie unter Solaris beispielsweise den Befehl **pkgadd**. Beantworten Sie während der Paketinstallation jede Eingabeaufforderung mit "yes".

So könnte eine typische Installation verlaufen:

```
# pkgadd -d RHATpossl-0.6-1.p24.6.pkg all
# pkgadd -d RHATpythn-2.4.1-2.rhn.4.sol9.pkg all
# pkgadd -d RHATrhnl-1.8-7.p23.pkg all
...
```

Anmerkung

Verwenden Sie die **-n** Option für **pkgadd** um den Befehl in einem nicht-interaktiven Modus auszuführen. Dies könnte allerdings dazu führen, dass die Installation einiger Pakete unter Solaris 10 unbemerkt scheitert.

Fahren Sie solange fort, bis jedes Paket in dem Red Hat Network-spezifischen Pfad installiert ist: **/opt/redhat/rhn/solaris/**.

2.1.3.1.5. Red Hat Network-Pakete in PATH einbinden

Um die Red Hat Network-Pakete bei jedem Login zugänglich zu machen, sollten Sie diese zu Ihrer PATH-Variable hinzufügen. Fügen Sie diesbezüglich diese Befehle zu Ihrem Login-Skript hinzu:

```
# PATH=$PATH:/opt/redhat/rhn/solaris/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/sbin
# export PATH
```

Um den Zugriff auf die Handbuchseiten (man-Seiten) der Befehle des Red Hat Network-Clients zu ermöglichen, fügen Sie diese zu Ihrer MANPATH-Variable hinzu. Fügen Sie hierfür die folgenden Befehle zu Ihrem Login-Skript hinzu:

```
# MANPATH=$MANPATH:/opt/redhat/rhn/solaris/man
# export MANPATH
```

Alternativ können Sie auch von der Befehlszeile aus mit folgendem Befehl auf die Handbuchseiten zugreifen:

```
# man -M /opt/redhat/rhn/solaris/man <man page>
```

Fügen Sie abschließend die Red Hat Bibliotheken zu Ihrer PATH-Variable hinzu, wie Sie es mit **libgcc**, **openssl** und **zlib** getan haben.

```
crle -c /var/ld/ld.config -l <current library paths>:/opt/redhat/rhn/solaris/lib
```

2.1.3.2. Implementieren der Client SSL-Zertifikate

Um die sichere Übertragung von Daten zu gewährleisten, empfiehlt Red Hat dringend die Verwendung von SSL. Der Red Hat Satellite vereinfacht die Implementation von SSL durch die Generierung der notwendigen Zertifikate während seiner Installation. Das serverseitige Zertifikat wird automatisch auf dem Satellite selbst installiert, während das Client-Zertifikat im Verzeichnis **/pub/** auf dem Web-Server des Satellites platziert wird.

Um das Zertifikat zu installieren, führen Sie diese Schritte für jeden Client durch:

1. Laden Sie das SSL-Zertifikat aus dem Verzeichnis **/var/www/html/pub/** des Red Hat Satellites auf das Client-System herunter. Das Zertifikat heißt **RHN-ORG-TRUSTED-SSL-CERT**, oder ähnlich. Es ist online unter der folgenden URL abrufbar: **https://your-satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT**.
2. Verschieben Sie das SSL-Zertifikat in das Red Hat Network spezifische Verzeichnis für Ihre UNIX-Variante. Unter Solaris erreicht man dies durch einen Befehl ähnlich dem Folgenden:

   ```
   mv /path/to/RHN-ORG-TRUSTED-SSL-CERT
   /opt/redhat/rhn/solaris/usr/share/rhn/
   ```

Nach Abschluss ist das neue Client-Zertifikat im entsprechenden Verzeichnis für Ihr UNIX-System installiert. Falls Sie eine große Anzahl von Systemen für das Red Hat Network-Management vorbereiten müssen, können Sie den gesamten Prozess als Skript erstellen.

Nun müssen Sie die Red Hat Network-Client-Applikationen noch so neu konfigurieren, dass diese auf das neue SSL-Zertifikat verweisen. Siehe Abschnitt 2.1.3.3, „Konfiguration der Clients“ für Anweisungen.

2.1.3.3. Konfiguration der Clients

Der letzte Schritt vor der Registrierung Ihrer Client-Systeme bei Red Hat Network ist die Neukonfiguration von deren Red Hat Network Applikationen, so dass diese das neue SSL-Zertifikat verwenden und Updates vom Red Hat Satellite erhalten. Beide Änderungen können durch das Bearbeiten der Konfigurationsdatei des **Red Hat Update Agent** durchgeführt werden, welche die Funktionalität für die Registrierung und das Update bietet.

Führen Sie diese Schritte auf jedem Client-System aus:

1. Wechseln Sie als Root in das Red Hat Network Konfigurations-Verzeichnis für das System. Unter Solaris lautet der vollständige Pfad **/opt/redhat/rhn/solaris/etc/sysconfig/rhn/**.
2. Öffnen Sie die **up2date**-Konfigurationsdatei in einem Texteditor.
3. Suchen Sie den Eintrag ***serverURL*** und setzen Sie dessen Wert auf den voll qualifizierten Domainnamen (FQDN) Ihres Red Hat Satellites:

   ```
   serverURL[comment]=Remote server URL
   serverURL=https://your-satellite.example.com/XMLRPC
   ```

4. Stellen Sie sicher, dass die Applikation auch bei Deaktivierung von SSL auf den Red Hat Satellite verweist, indem Sie außerdem den Wert ***noSSLServerURL*** auf den Satellite setzen:

   ```
   noSSLServerURL[comment]=Remote server URL without SSL
   noSSLServerURL=http://your-satellite.example.com/XMLRPC
   ```

5. Suchen Sie bei noch geöffneter **up2date**-Konfigurationsdatei den Eintrag ***sslCACert*** und setzen Sie dessen Wert auf den Namen und den Ort des SSL-Zertifikats, wie in Abschnitt 2.1.3.2, „Implementieren der Client SSL-Zertifikate“ beschrieben. Zum Beispiel:

```
sslCACert[comment]=The CA cert used to verify the ssl server
sslCACert=/opt/redhat/rhn/solaris/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

Ihre Client-Systeme sind nun bereit für die Registrierung beim Red Hat Network und für die Verwaltung durch Ihren Satellite.

2.1.4. Registrierung und Updates für Unix-Clients

Nachdem Sie nun Red Hat Network-spezifische Pakete installiert, SSL implementiert und Ihre Client-Systeme dahingehend rekonfiguriert haben, dass diese sich mit dem Red Hat Satellite verbinden, können Sie mit der Registrierung von Systemen beginnen und Updates erhalten.

2.1.4.1. Registrieren von Unix-Systemen

Dieser Abschnitt beschreibt den Red Hat Network Registrierungs-Prozess für UNIX-Systeme. Dazu müssen Sie **rhnreg_ks** verwenden; die Verwendung von Aktivierungsschlüsseln zur Registrierung Ihrer Systeme ist optional. Diese Schlüssel ermöglichen es Ihnen, Einstellungen im Red Hat Network vorzubestimmen, wie beispielsweise Basis-Channels und Systemgruppen und diese zum Zeitpunkt der Registrierung automatisch auf den entsprechenden Systemen anzuwenden.

Da die Erstellung von Aktivierungsschlüsseln und deren Verwendung weitgehend in anderen Handbüchern behandelt wird, konzentriert sich dieser Abschnitt auf Unterschiede bei deren Anwendung auf UNIX-Varianten.

Um UNIX-Systeme mit Ihrem Red Hat Satellite zu registrieren, führen Sie folgende Aufgaben in dieser Reihenfolge durch:

1. Melden Sie sich auf der Weboberfläche des Satellite an und klicken Sie den **Systeme** Tab in der oberen Navigationsleiste und danach **Aktivierungsschlüssel** in der linken Navigationsleiste. Klicken Sie dann den Link **Neuen Schlüssel erstellen** ganz rechts oben auf der Seite.
2. Wählen Sie auf der folgenden Seite den Basis-Channel, den Sie am Ende von Abschnitt 2.1.2, „Satellite Server Vorbereitung/Konfiguration“ erstellt haben.
3. Nachdem Sie den Schlüssel erzeugt haben, klicken Sie auf dessen Namen in der **Aktivierungsschlüssel** Liste und erweitern dessen Red Hat Network Einstellungen, indem Sie Software und Konfigurations-Channel und Systemgruppen verknüpfen.
4. Öffnen Sie ein Terminal auf dem zu registrierenden Client-System und wechseln Sie zum Root-Benutzer.
5. Verwenden Sie **rhnreg_ks** zusammen mit der Option **--activationkey**, um den Client beim Satellite zu registrieren. Die Zeichenkette, die den Schlüssel bildet, kann direkt von der **Aktivierungsschlüssel**-Liste auf der Website kopiert werden. Der Befehl sieht dann ungefähr so aus:

```
rhnreg_ks --activationkey=b25fef0966659314ef9156786bd9f3af
```

6. Gehen Sie zurück auf die Website und klicken Sie auf den Namen des Aktivierungsschlüssels und überprüfen Sie, ob das neue System im **Aktivierte Systeme** Tab erscheint.

2.1.4.2. Beziehen von Updates

Paket-Updates werden unter UNIX anders abgewickelt als unter Linux. Beispielsweise benötigt Solaris

Patch-Clusters, um mehrere Pakete auf einmal zu aktualisieren. Red Hat Betriebssysteme verwenden hingegen Errata-Updates, um Upgrades mit spezifischen Paketen in Verbindung zu bringen. Zusätzlich dazu verwendet Solaris sogenannte Antwort-Dateien, um interaktive Paket-Installationen zu automatisieren. Dies findet bei Linux keine Anwendung. Red Hat bietet dazu das Konzept von Quellpaketen an. Aus diesem Grund wird in diesem Abschnitt versucht, die Unterschiede bei der Verwendung von Red Hat Network-Tools auf UNIX-Systemen hervorzuheben. (Hinweis: Solaris Antwort-Dateien werden von Red Hat Network derzeit nicht unterstützt; dies ist jedoch für zukünftige Releases geplant.)

Trotz der Unterschiede, wie beispielsweise dem Fehlen von Errata, weisen die Channel- und Paket-Management-Oberflächen auf der Red Hat Network-Website auf dem Satellite größtenteils die gleichen Funktionen für UNIX-Systeme auf. Alle Software-Channels für UNIX-Varianten können beinahe auf die gleiche Weise erstellt werden, wie die benutzerdefinierten Channels, die im *Red Hat Satellite Getting Started Guide (Einführungshandbuch)* genauer behandelt werden. Der signifikanteste Unterschied ist die Architektur. Wenn Sie einen UNIX-Software-Channel erstellen, müssen Sie unbedingt die entsprechende Basis-Channel-Architektur auswählen.

Unterteilen Sie die Pakete je nach Beschaffenheit in Basis- und Sub-Channels. Beispielsweise sollten auf Solaris die Installationspakete in den Solaris-Basis-Channel kommen und Patches und Patch-Clusters in einen Sub-Channel des Solaris Basis-Channels. Extra-Installationspakete sollten in einen separaten Extras Sub-Channel gelangen.

Red Hat Network behandelt Patches ähnlich wie Pakete; diese werden auf dieselbe Art und mit demselben Interface wie normale Pakete aufgelistet und installiert. Patches werden von Solaris 'nummeriert' und besitzen Namen wie z.B. "patch-solaris-108434". Die Version eines Solaris-Patch wird den originalen Solaris-Metadaten entnommen, wobei die Release immer 1 ist.

Patch-Cluster sind ein Bündel von Patches, die als eine Einheit installiert werden. Red Hat Network beobachtet immer, wann zuletzt ein Patch-Cluster auf einem System installiert worden ist. Diese erscheinen jedoch niemals in der Liste der auf dem System installierten Pakete, sogar nachdem diese installiert worden sind. Patch-Cluster-Namen lesen sich wie z. B. "patch-cluster-solaris-7_Recommended". Die Version ist eine Datumszeichenfolge wie beispielsweise "20040206", die Release ist immer 1 und der Zeitraum ist immer 0.

2.1.4.2.1. Hochladen der Pakete auf den Satellite

Red Hat Network liefert keinen UNIX-Inhalt; alle Solaris-Pakete, Patches oder Patch-Cluster müssen von einem Client-System auf den Satellite in einem Format hochgeladen werden, das dieser versteht. Das Paket kann anschließend verwaltet und an andere Systeme verteilt werden. Red Hat Network kreierte **`solaris2mpm`** um Solaris-Pakete, Patches und Patch-Cluster in ein Format zu übersetzen, das der Satellite verstehen kann.

2.1.4.2.1.1. `solaris2mpm`

Wie kurz in Abschnitt 2.1.1.4, „Unterschiede in der Funktionalität“ erwähnt, ist **`solaris2mpm`** Teil von Red Hat Network Push für Solaris. Der Inhalt, der auf einen Solaris-Channel auf dem Satellite gepusht wird, muss zunächst im Format ".mpm" vorliegen.

Eine .mpm-Datei ist ein Archiv, das eine Beschreibung der Paketdaten, sowie des Pakets oder Patches selbst enthält. Der solaris2mpm-Befehl muss auf dem Client ausgeführt werden, niemals auf dem Satellite.

Anmerkung

solaris2mpm benötigt den dreifachen Platz eines Paketes, Patches oder Patch-Clusters, das es konvertiert. Normalerweise wird der Platz in **/tmp/** zu diesem Zweck verwendet. Mit der Option **--tempdir** kann jedoch, falls notwendig, ein anderes Verzeichnis angegeben werden.

Auf der Befehlszeilenebene von solaris2mpm können mehrere Dateien angegeben werden. Nachstehend finden Sie ein Anwendungsbeispiel:

```
# solaris2mpm RHATrpush-3.1.5-21.pkg RHATrpush-3.1.5-23.pkg
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-21.sparc-solaris.mpm
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-23.sparc-solaris.mpm
```

Da kein anderes Verzeichnis angegeben wurde, werden die resultierenden .mpm-Dateien in das Verzeichnis /tmp/ geschrieben. Beachten Sie bitte, dass der Name der resultierenden .mpm-Dateien den Namen der Architektur des Clients, auf dem sie kreiert wurden, beinhaltet. In diesem Falls war dies SPARC Solaris. Das allgemeine Format von .mpm-Dateinamen ist:

```
name-version-release.arch.mpm
```

Patch-Cluster sind "explodierte" - .mpm-Dateien, die für jeden Patch im Cluster generiert wurden. Weiterhin existiert eine "Meta"-.mpm-Datei auf höchster Ebene, die Informationen über den Cluster als Ganzes enthält.

Nachfolgend sehen Sie die solaris2mpm-Optionen:

Tabelle 2.2. solaris2mpm-Optionen

Option	Beschreibung
--version	Zeigt die Versionsnummer des Programms an und beendet
-h, --help	Zeigt diese Information an und beendet
-?, --usage	Gibt Informationen zur Verwendung des Programms an und beendet
--tempdir=<tempdir>	Temporäres Arbeitsverzeichnis
--select-arch=<arch>	Wählt die Architektur (i386 oder SPARC) für multi-arch-Pakete.

2.1.4.2.1.2. rhnpush mit .mpm-Dateien

Die Solarisversion von **rhnpush** funktioniert wie ein Standard-Hilfsprogramm mit der zusätzlichen Fähigkeit, mit .mpm-Dateien umzugehen. Nachfolgend ist ein Anwendungsbeispiel aufgeführt:

```
% rhnpush -v --server testbox.example.com --username myuser -c solaris-8 \
RHATrpush-3.1.5-*.mpm
 Red Hat Network password:
 Connecting to http://testbox.example.com/APP
 Uploading package RHATrpush-3.1.5-21.sparc-solaris.mpm
 Uploading package RHATrpush-3.1.5-23.sparc-solaris.mpm
```

Anmerkung

Patch-Cluster .mpm-Dateien müssen entweder gleichzeitigt, oder nach - niemals vor - den .mpm-Dateien für die Patches, die in diesem Cluster enthalten sind, gepusht werden.

Verwenden Sie solaris2mpm auf jedem der Pakete, Patches oder Patch-Cluster, die Sie via Satellite verwalten möchten. Verwenden Sie anschließend Red Hat Network Push, um sie in den Channel hochzuladen, den Sie dafür erstellt haben.

2.1.4.2.2. Durch die Website aktualisieren

Um Pakete oder Patches auf einem individuellen System zu installieren, klicken Sie den Namen des Systems in der **Systeme** Kategorie, wählen die Pakete von den Upgrade- oder Installations-Listen des **Pakete** oder **Patches** Tab aus und klicken **Ausgewählte Pakete installieren/aktualisieren**.

Um während der Installation einen Remote-Befehl auszuführen, klicken Sie auf **Remote-Befehl ausführen** statt auf **Bestätigen**. Siehe Abschnitt 2.1.5, „Remote-Befehle“ für Instruktionen.

Um Pakete oder Patches auf mehreren Systemen auf einmal zu installieren, wählen Sie die Systeme aus und klicken Sie **System-Set-Manager** in der linken Navigationsleiste. Auf dem **Pakete** Tab wählen Sie dann die Pakete von den Upgrade- oder Installations-Listen aus und klicken **Pakete installieren/aktualisieren**. Schlussendlich planen Sie die Updates ein.

2.1.4.2.3. rhnsd

Auf Red Hat Enterprise Linux Systemen startet der **rhnsd**-Daemon, der die Client-Systeme anweist, sich bei Red Hat Network anzumelden, automatisch zum Zeitpunkt des Bootens. Auf Solaris-Systemen startet der **rhnsd** standardmäßig *nicht* automatisch zum Zeitpunkt des Bootens. Er kann wie folgt von der Befehlszeile aus gestartet werden:

```
rhnsd --foreground --interval=240
```

Der standardmäßige Ort für den **rhnsd** ist **/opt/redhat/rhn/solaris/usr/sbin/rhnsd**. Nachfolgend sind die verfügbaren Optionen für den **rhnsd** unter Solaris aufgeführt:

Tabelle 2.3. rhnsd Optionen

Option	Beschreibung
-f, --foreground	Im Vordergrund laufen
-i, --interval=MINS	Alle MINS Minuten mit dem Red Hat Network verbinden
-v, --verbose	Alle Aktionen im Syslog protokollieren
-h, --help	Diese Hilfeliste anbieten
-u, --usage	Diese Hilfeliste anbieten
-V, --version	Programmversion ausgeben

2.1.4.2.4. Von der Befehlszeile aus aktualisieren

Wie die Website ist auch die Verwendung des **Red Hat Update Agents** via Befehlszeile von den Einschränkungen des UNIX-Paketmanagement betroffen. Die meisten Kernfunktionen können jedoch

immer noch mithilfe des **up2date** Befehls durchgeführt werden. Der signifikanteste Unterschied ist das Fehlen aller Optionen in Bezug auf Quelldateien. Siehe Tabelle 2.4, „Befehlszeilenparameter des Update Agenten“ für eine genaue Liste der Optionen, die für UNIX-Systeme zur Verfügung stehen.

Die Befehlszeilenversion des **Red Hat Update Agents** akzeptiert folgende Parameter auf UNIX-Systemen:

Tabelle 2.4. Befehlszeilenparameter des Update Agenten

Parameter	Beschreibung
--version	Zeige Information zu Programmversion.
-h, **--help**	Zeige Hilfe-Text und beende.
-v, **--verbose**	Zeige zusätzlichen Output.
-l, **--list**	Liste die neuesten Versionen aller installierten Pakete.
-p, **--packages**	Aktualisiere Pakete in Zusammenhang mit diesem System-Profil.
--hardware	Aktualisiere das Hardware-Profil dieses Systems auf Red Hat Network.
--showall	Liste alle zum Herunterladen verfügbaren Pakete.
--show-available	Liste alle verfügbaren Pakete, die derzeit nicht installiert sind.
--show-orphans	Liste alle derzeit installierten Pakete, die sich nicht in Channels befinden auf die das System subskribiert ist.
--show-channels	Zeige die Channel-Namen gemeinsam mit den Paketnamen.
--installall	Installiere alle verfügbaren Pakete. Verwende mit der **--channel** Option.
--channel=*CHANNEL*	Geben Sie an, von welchen Channels unter Verwendung von Channel-Labels aktualisiert werden soll.
--get	Rufen Sie das festgelegte Paket ab, ohne dabei Abhängigkeiten aufzulösen.

2.1.5. Remote-Befehle

Mit UNIX-Unterstützung bietet Red Hat Network die Flexibilität, Remote-Befehle auf Client-Systemen mittels der Website des Satellites auszuführen. Dieses Feature ermöglicht es Ihnen nahezu jede (kompatible) Applikation oder jedes Skript auf jedem System in Ihrer Domain laufen zu lassen, ohne jemals wieder ein Terminal öffnen zu müssen.

2.1.5.1. Befehle aktivieren

Mit der gewonnen Flexibilität ist jedoch auch ein großes Risiko verbunden und die Verantwortung, dieses Risiko so gering als möglich zu halten. Jeder mit administrativem Zugang zum System auf der Website erhält eine Root-BASH-Befehlszeile.

Dies kann jedoch durch dieselben config-enable-Mechanismen gesteuert werden, mit denen die Systeme ermittelt werden, deren Konfigurations-Dateien von Red Hat Network verwaltet werden können.

Kurz gesagt müssen Sie ein Verzeichnis und eine Datei auf dem UNIX-System erstellen, das dem Red Hat Network anzeigt, dass das Ausführen von Remote-Befehlen auf dem Rechner akzeptabel ist. Das Verzeichnis muss **script** genannt werden, die Datei **run**, und beide müssen sich im **/etc/sysconfig/rhn/allowed-actions/** Verzeichnis befinden (spezifisch zu Ihrer UNIX-

Variante).

In Solaris führen Sie beispielsweise folgenden Befehl aus, um das Verzeichnis zu erstellen:

```
mkdir -p /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-actions/script
```

Um die Datei in Solaris zu erstellen, führen Sie folgenden Befehl aus:

```
touch /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-actions/script/run
```

2.1.5.2. Befehle ausführen

Sie können einen Remote-Befehl auf viele Arten einplanen: auf einem individuellen System, auf einmal auf mehreren Systemen und um eine Paket-Aktion zu begleiten.

Um einen Remote-Befehl auf einem einzelnen System auszuführen, öffnen Sie die **System-Details** Seite, klicken den **Remoter Befehl** Sub-Tab (Beachten Sie, dass dieser Sub-Tab nur erscheint, wenn das System über eine Provisioning-Berechtigung verfügt.) und legen die Einstellungen für den Befehl fest. Sie können einen bestimmten Benutzer, eine bestimmte Gruppe und Zeitablauf-Periode festlegen sowie auch das Skript selbst. Wählen Sie das Datum und die Zeit, den Befehl zu beginnen zu versuchen, aus und klicken den **Remoten Befehl einplanen** Link.

Auf eine ähnliche Weise können Sie einen Remote-Befehl auf mehreren Systemen auf einmal mit dem **System Set Manager** ausführen. Wählen Sie die Systeme aus, gehen zum **System Set Manager**, klicken den **Provisioning** Tab und scrollen zum Abschnitt **Remote-Befehl** hinunter. Von dort können Sie einen Remote-Befehl gleichzeitig auf allen ausgewählten Systemen ausführen.

Um einen Remote-Befehl mit einer Paket-Aktion laufen zu lassen, planen Sie die Aktion mittels dem **Pakete** Tab der **System-Details** Seite und klicken **Remoten Befehl ausführen**, wobei gleichzeitig die Aktion bestätigt wird. Verwenden Sie dazu die Radio-Buttons ganz oben um festzulegen, ob der Befehl vor oder nach der Paket-Aktion laufen soll, legen die Einstellungen für den Befehl fest und klicken **Paket-Installation/Upgrade planen**.

Beachten Sie, dass die Installation von mehreren Paketen, die unterschiedliche Remote-Befehle besitzen, es erfordert, dass Sie die Installationen separat einplanen oder die Befehle zu einem einzigen Skript zusammenlegen.

Kapitel 3. Red Hat Satellite Proxy Information

Dies ist ein Abschnitt über die Verwendung von Red Hat Satellite Proxy mit dem Red Hat Network Package Manager.

3.1. Verwendung des Red Hat Network Package Manager und die Lieferung Lokaler Pakete mittels Red Hat Network Proxy

Der Red Hat Network Package Manager ist ein Befehlszeilen-Tool, durch das eine Organisation lokale Pakete mit einem privaten Red Hat Network-Channel durch den Red Hat Network Proxy Server betreuen kann. Installieren Sie den Red Hat Network Package Manager nicht um nur offizielle Red Hat-Pakete für den Red Hat Network Proxy Server zu aktualisieren.

Um den Red Hat Network Package Manager zu verwenden, installieren Sie das **`spacewalk-proxy-package-manager`** Paket samt aller Abhängigkeiten.

Es wird nur die Header-Information für Pakete auf die Red Hat Network Server hochgeladen. Die Header werden dazu benötigt, um Red Hat Network das Auflösen von Paketabhängigkeiten für die Client-Systeme zu ermöglichen. Die eigentlichen Paketdateien (**`*.rpm`**) befinden sich auf dem Red Hat Network Proxy Server.

Der Red Hat Network Package Manager verwendet dieselben Einstellungen wie der Proxy, die in der **`/etc/rhn/rhn.conf`** Konfigurations-Datei festgelegt sind.

Sehen Sie im Folgenden eine Zusammenfassung aller Befehlszeilen-Optionen für den Red Hat Network Package Manager **`rhn_package_manager`**:

Tabelle 3.1. Optionen für `rhn_package_manager`

Option	Beschreibung
-v, **--verbose**	Ausführlichkeit der Ausgabe erhöhen.
-d*DIR*, **--dir=*DIR***	Verarbeitet die Pakete des Verzeichnisses ***DIR***.
-c*CHANNEL*, **--channel=*CHANNEL***	Verwaltet diesen Channel - kann auch mehrmals vorhanden sein.
-n*NUMBER*, **--count=*NUMBER***	Verarbeitet diese Anzahl von Headern pro Aufruf - Standard ist 32.
-l, **--list**	Listet jeden Paketnamen, jede Versionsummer, Release-Nummer und Architektur in den festgelegten Channels/im Channel auf.
-s, **--sync**	Überprüft, ob lokales Verzeichnis mit dem Server abgestimmt (synchron) ist.
-p, **--printconf**	Zeigt die aktuelle Konfiguration an und beendet.
-X*PATTERN*, **--exclude=*PATTERN***	Schließt Dateien aus, die diesem globalen Ausdruck entsprechen - kann auch mehrmals vorhanden sein.
--newest	Sende nur die Pakete, die neuer sind als die bereits für den festgelegten Channel zum Server gesendeten Pakete.
--stdin	Liest die Paketnamen von der Standardeingabe.
--nosig	Sende nicht-signierte Pakete. Standardmäßig versucht der Red Hat Network Package Manager nur signierte Pakete zu senden.
--username=*USERNAME*	Geben Sie Ihren Red Hat Network Benutzernamen ein. Wenn Sie mit dieser Option keinen Benutzernamen angeben, dann werden Sie dazu aufgefordert.
--password=*PASSWORD*	Geben Sie Ihr Red hat Network Passwort ein. Wenn Sie mit dieser Option kein Passwort angeben, dann werden Sie dazu aufgefordert.
--source	Lädt Quellpaket-Header hoch.
--dontcopy	Nach dem Hochladen werden die Pakete nicht automatisch in den Paketbaum kopiert.
--test	Zeigt nur die zu sendenden Pakete an.
--no-ssl	*Nicht empfohlen* - SSL abschalten.
-?, **--usage**	Beschreibt kurz die Optionen.
--copyonly	Kopiert die als Parameter angegebene Datei in den angegebenen Channel. Nützlich, wenn einem Channel auf dem Proxy ein Paket fehlt und Sie nicht alle Pakete im Channel nochmals importieren möchten. Beispielsweise: **`rhn_package_manager -c`*`CHANNEL`*`--copyonly`*`/PATH/TO/MISSING/FILE`**
-h, **--help**	Zeigt den Hilfebildschirm mit einer Liste von Optionen an.

Tip

Diese Befehlszeilenoptionen sind auch auf der **rhn_package_manager** man-Seite aufgeführt: **man rhn_package_manager**.

Damit Red Hat Network Package Manager in der Lage ist die lokalen Pakete zu senden müssen die folgenden Schritte beachtet werden:

1. Einrichten eines privaten Channels.
2. Laden der lokalen Pakete in the Channel.

Die Schritte werden in den folgenden Abschnitten weiter besprochen.

3.1.1. Erstellen eines Privaten Channels

Bevor lokale Pakete durch den Red Hat Network Proxy Server bereitgestellt werden können, benötigen Sie einen privaten Channel zur Aufbewahrung. Führen Sie folgende Schritte durch, um einen privaten Channel einzurichten:

1. Melden Sie sich über die Red Hat Network Weboberfläche bei https://rhn.redhat.com oder auf dem lokalen Red Hat Satellite Server im Netzwerk an.
2. Klicken Sie auf **Channels** auf der oberen Navigationsleiste. Wenn die **Channels verwalten** Option nicht in der linken Navigationsleiste erscheint, dann versichern Sie sich, dass dieser Benutzer über die Berechtigungen zur Channel-Bearbeitung verfügt. Gehen Sie dazu zur **Benutzer** Kategorie, die über die obere Navigationsleiste zugänglich ist.
3. In der linken Navigationsleiste klicken Sie **Software Channels verwalten** und dann die **Neuen Channel erstellen** Schaltfläche ganz rechts oben auf der Seite.
4. Wählen Sie eine Parent-Channel- und Basis-Channel-Architektur aus und geben dann Name, Label, Zusammenfassung und Beschreibung für den neuen privaten Channel ein. Das Label muss mindestens sechs Zeichen lang sein, mit einem Buchstaben beginnen und darf nur Kleinbuchstaben, Zahlen, Bindestriche (-) und Punkte(.) enthalten. Geben Sie auch die URL des GPG-Schlüssels des Channels ein. Obwohl dies kein zwingend erforderliches Feld ist, wird es empfohlen, um die Sicherheit zu erhöhen. Siehe *Red Hat Network Channel-Managementhandbuch* für eine Anleitung zur Herstellung von GPG-Schlüsseln.
5. Klicken Sie auf **Channel erstellen**.

3.1.2. Hochladen von Paketen

Anmerkung

Sie müssen ein Organisations-Administrator sein, um Pakete auf private Red Hat Network Channels hochladen zu können. Das Skript fragt Sie nach Ihrem Red Hat Network Benutzernamen und Passwort.

Nach dem Einrichten des privaten Channels können Sie die Paket-Header für Ihre Binär- und Quellen-RPMs auf den Red Hat Network Server hochladen und die Pakete zum Red Hat Network Proxy Broker Server kopieren. Um die Paket-Header für die Binär-RPMs hochzuladen, geben Sie folgendes in der Befehlszeile ein:

```
rhn_package_manager -c "label_of_private_channel" pkg-list
```

Dieser Befehl ladet den Header des Pakets in den angegebenen Channel, und das Paket selbst in **/var/spool/rhn-proxy/rhn**.

pkg-list ist die Liste der hochzuladenden Pakete. Wahlweise können Sie auch die **-d** Option verwenden, um das lokale Verzeichnis festzulegen, welches die zum Channel hinzuzufügenden Pakete enthält. Vergewissern Sie sich, dass dieses Verzeichnis nur die benötigten Pakete enthält und keine anderen Dateien. Der Red Hat Network Package Manager kann die Liste von Paketen auch von der Standardeingabe lesen (unter Verwendung von **--stdin**).

Um die Paket-Header für die Quellen-RPMs hochzuladen:

```
rhn_package_manager -c "label_of_private_channel" --source pkg-list
```

Wenn Sie mehr als einen Channel angegeben haben (unter Verwendung der **-c** oder **--channel** Option), werden die hochgeladenen Paket-Header mit allen aufgelisteten Channels verknüpft.

Anmerkung

Wenn kein Channel-Name angegeben wird, werden die Pakete zu keinem Channel hinzugefügt. Die Pakete können dann einem Channel mit Hilfe der Red Hat Network Weboberfläche hinzugefügt werden. Das Interface kann auch zur Modifizierung bestehender privater Channels verwendet werden.

Nach dem Hochladen der Pakete können Sie sofort auf der Red hat Network Weboberfläche überprüfen, ob diese aufgelistet sind. Klicken Sie auf **Channels** in der oberen Navigationsleiste, auf **Software-Channels verwalten** in der linken Navigationsleiste und dann auf den Namen des benutzerdefinierten Channels. Klicken Sie dann auf den **Pakete** Unter-Tab. Jedes RPM-Paket sollte aufgelistet sein.

Sie können auch mit Hilfe der Befehlszeile überprüfen, ob das lokale Verzeichnis mit dem Image der Channels des Red Hat Network Servers übereinstimmt:

```
rhn_package_manager -s -c "label_of_private_channel"
```

Die **-s** Option listet alle fehlenden Pakete (Hochgeladene Pakete auf dem Red Hat Network Server, die nicht im lokalen Verzeichnis vorhanden sind). Sie müssen ein Organisations-Administrator sein, um diesen Befehl verwenden zu können. Das Skript verlangt Ihren Red Hat Network Benutzernamen und das Passwort.

Wenn Sie den Red Hat Network Package Manager dazu verwenden, lokale Pakete hochzuladen, müssen Sie dazu auf die Red Hat Network Website gehen, um das System beim privaten Channel anzumelden.

Kapitel 4. Verwaltung von benutzerdefinierten Paketen

Dieses Kapitel gibt einen Überblick über das Erstellen von Paketen zur erfolgreichen Auslieferung via Red Hat Network. Dabei wird unter anderem darauf eingegangen, warum RPM verwendet werden sollte, wie Pakete für Red hat Network erstellt werden sollten und wie Pakete richtig signiert werden können.

4.1. Erstellen von Paketen für Red Hat Network

Red Hat Network verwendet die *RPM Paketmanager* (RPM) Technologie, um festzustellen, welche zusätzliche Software und Updates auf jedes Client-System anwendbar sind. Pakete, die von Red Hat Network abgerufen werden, liegen üblicherweise im RPM-Format vor. ISO-Images sind dagegen über den **`Software`** Tab auf der Red Hat Network Website erhältlich, sind jedoch nicht für Red Hat Satellite Installationen verfügbar. Wenn Ihr Satellite-Server Solaris-Support aktiviert hat, können Sie Red Hat Network Push dazu verwenden, Solaris-Pakete in benutzerdefinierte Channels hochzuladen, die von Solaris-Clients verwendet werden.

RPM ist ein Tool, welches das Installieren, Deinstallieren, Aktualisieren und Verifizieren von Software-Paketen erleichtern soll. Software-Entwickler können damit auch den Quellcode und die kompilierte Version eines Programms für Endbenutzer und Entwickler verpacken.

4.1.1. Vorteile von RPM

RPM hat folgende Vorteile:

Einfache Aktualisierungen

Durch die Verwendung von RPM aktualisieren Sie individuelle Komponenten eines Systems, ohne dabei komplett neu installieren zu müssen. Wenn Red Hat eine neue Version von Red Hat Enterprise Linux veröffentlicht, müssen Benutzer nicht von Grund auf neu installieren. RPM ermöglicht 'intelligente' und vollautomatische Aktualisierungen Ihres Systems. Konfigurationsdateien in Paketen gehen nicht während der Aktualisierungen verloren. Benutzer verlieren daher keine benutzerspezifischen Anpassungen. Es werden keine speziellen Aktualisierungsdateien benötigt, um ein Paket zu aktualisieren, da dieselbe RPM-Datei dazu benutzt wird, das Paket zu installieren und zu aktualisieren.

Paketabfragen

RPM bietet Abfrageoptionen, um die gesamte RPM-Datenbank nach allen Paketen oder auch nur nach bestimmten Dateien zu durchsuchen. Sie können auch auf einfachste Weise den Ursprung des Pakets und zu welchem Paket eine Datei gehört herausfinden. Die Dateien im Paket befinden sich in einem komprimierten Archiv mit einem speziellen Binär-Header, der nützliche Informationen über das Paket und dessen Inhalte enthält. RPM durchsucht die Header auf rasche und einfache Weise.

Systemverifizierung

Ein weiteres Feature ist die Paketverifizierung. Wenn Sie glauben, dass eine Datei eines Pakets versehentlich gelöscht wurde, können Sie das Paket durchsehen und den Status der darin enthaltenen Dateien überprüfen. Diese Verifizierung benachrichtigt Sie über alle Besonderheiten. Wenn ein Fehler vorhanden ist, können Sie die Dateien auf einfachste Weise nochmals installieren. Modifizierte Konfigurationsdateien werden während der Neuinstallation nicht verändert.

Unverfälschte Quellen

Ein äußerst wichtiges Merkmal von RPM ist die Möglichkeit der Verwendung *unverfälschter*

Software-Quellen, wie Sie von den ursprünglichen Autoren herausgegeben wurden. Mit RPM können die ursprünglichen Quellen-Dateien gemeinsam mit allen verwendeten Patches und den kompletten Build-Instruktionen paketiert werden. Dies ist aus mehreren Gründen wichtig. Wenn nämlich beispielsweise eine neue Version eines Programms herausgegeben wird, müssen Sie nicht unbedingt wieder ganz von vorne anfangen, um es zu kompilieren. Sie können sich den Patch ansehen und dann eine Entscheidung darüber treffen, was Sie *vielleicht* unternehmen sollten. Alle mitkompilierten Standards und Änderungen, die einen einwandfreien Build gewährleisten sollen, können mithilfe dieser Technik auf einfache Weise sichtbar gemacht werden.

Quellen unverfälscht zu erhalten mag nur für Entwickler wichtig erscheinen, resultiert jedoch letztendlich auch in einer besseren Software-Qualität für den Endbenutzer.

4.1.2. Red Hat Network RPM-Richtlinien

Die Stärke von RPM liegt in der Fähigkeit, Abhängigkeiten zu bestimmen und Konflikte richtig zu identifizieren. Red Hat Network verlässt sich auf diesen Aspekt von RPM. Red Hat Network bietet eine automatisierte Umgebung, was bedeutet, dass kein manueller Eingriff während der Installation eines Pakets stattfinden kann. Wenn daher RPMs zur Verteilung durch Red Hat Network erstellt werden, ist es zwingend notwendig, sich an folgende Regeln zu halten:

1. Erwerben Sie RPM-Kenntnisse. Es ist äußerst wichtig, ein fundamentales Verständnis der wichtigen Features von RPM zu besitzen, um Pakete richtig erstellen zu können. Für nähere Information verweisen wir für den Anfang auf folgende Informationsquellen:
   - http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html
   - http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/Packagers_Guide/index.html
   - http://www.gurulabs.com/GURULABS-RPM-LAB/GURULABS-RPM-GUIDE-v1.0.PDF
2. Wenn Sie eine RPM-Datei für einen Sub-Channel erstellen, dann erstellen Sie das Paket auf einer 'frischen' Installation von Red Hat Enterprise Linux mit derselben Version, wie der Basis-Channel des Sub-Channels. Stellen Sie sicher, dass Sie zuerst alle Updates von Red Hat Network anwenden.
3. Das RPM-Paket muss ohne Verwendung der Optionen **`--force`** oder **`--nodeps`** installiert werden können. Wenn Sie ein RPM auf Ihrem Build-System nicht sauber installieren können, dann kann dieses auch von Red Hat Network nicht automatisch auf einem System installiert werden.
4. Der Dateiname des RPM-Pakets muss dem NVR-Format (Name, Version, Release) entsprechen und die Architektur für das Paket beinhalten. Das richtige Format ist ***`name-version-release.arch`*`.rpm`**. Beispielsweise ist **`pkgname-0.84-1.i386.rpm`** ein gültiger Dateiname für ein RPM-Paket, wobei ***`pkgname`*** der Paketname ist, ***`0.84`*** die Version, ***`1`*** das Release und ***`i386`*** die Architektur.
5. Das RPM-Paket sollte vom Maintainer des Pakets signiert werden. Nicht signierte Pakete können zwar über das Red Hat Network verteilt werden, jedoch muss **yum** dazu gezwungen werden, diese zu akzeptieren. Das Signieren von Paketen wird dringend empfohlen und wird in Abschnitt 4.2, „Digitale Signaturen für Red Hat Network Pakete“ im Detail behandelt.
6. Wenn die Version in irgendeiner Form verändert wird, inklusive Änderung der Signatur oder Neukompilierung, muss die Version oder das Release inkrementell erhöht werden. Mit anderen Worten muss die NVRA (inkl. Architektur) für jedes RPM, das durch Red Hat Network verteilt wird, einem individuellen Build entsprechen, um Unklarheiten zu vermeiden.
7. Kein RPM-Paket darf sich selbst als veraltet kennzeichnen.

8. Wenn ein Paket in separate Pakete aufgeteilt wird, dann sollten Sie extrem vorsichtig mit den Abhängigkeiten sein. Teilen Sie kein bestehendes Paket auf, wenn nicht ein zwingender Grund dazu besteht.
9. Kein Paket darf auf interaktive Pre-Installations-, Post-Installations, Pre-Deinstallations oder Post-Deinstallations-Skripte angewiesen sein. Wenn das Paket einen direkten Benutzereingriff während der Installation benötigt, funktioniert es nicht mit Red Hat Network.
10. Jegliche Pre-Installations-, Post-Installations, Pre-Deinstallations oder Post-Deinstallations-Skripte sollten niemals etwas auf Standardfehler (stderr) oder Standardausgabe (stoud) ausgeben. Lenken Sie die Mitteilungen auf **`/dev/null`** um, wenn sie nicht notwendig sind. Andernfalls schreiben Sie diese in eine Datei.
11. Wenn Sie die spec-Datei erstellen, verwenden Sie die Gruppendefinitionen von **`/usr/share/doc/rpm-<version>/GROUPS`**. Wenn Sie keine genaue Übereinstimmung finden, dann wählen Sie den nächstbesten Treffer aus.
12. Verwenden Sie das RPM-Abhängigkeiten-Feature um sicherzugehen, dass das Programm auch nach der Installation läuft.

Wichtig

Erstellen Sie kein RPM, indem Sie Dateien archivieren und diese dann im Post-Installationsskript wieder dearchivieren. Dies entspricht in keiner Weise dem Zweck von RPMs.

Wenn die Dateien im Archiv nicht in der Dateiliste enthalten sind, dann können diese nicht auf Konflikte hin überprüft werden. In den meisten Fällen kann RPM selbst Archive am effektivsten packen und entpacken. Erstellen Sie beispielsweise keine Dateien in %post, die Sie nicht in einer %postun Sektion entfernen können.

4.2. Digitale Signaturen für Red Hat Network Pakete

Alle Pakete, die durch Red Hat Network verteilt werden, sollten eine *digitale Signatur* besitzen. Diese besteht aus einem einzigartigen, privaten Schlüssel und kann mit dem dazugehörigen öffentlichen Schlüssel verifiziert werden. Nachdem ein Paket erstellt wurde, können die SRPM (Source-RPM) und die RPM-Pakete digital mit einem GnuPG-Schlüssel signiert werden. Bevor das Paket installiert wird, wird mithilfe des öffentlichen Schlüssels festgestellt, ob das Paket von einer vertrauenswürdigen Partei signiert wurde und in der Zwischenzeit auch nicht verändert wurde.

4.2.1. GnuPG-Schlüsselpaar generieren

Ein GnuPG-Schlüsselpaar besteht aus dem privaten und dem öffentlichen Schlüssel. Um ein Schlüsselpaar zu erstellen:

1. Geben Sie den folgenden Befehl als Root am Shell-Prompt ein:

   ```
   gpg --gen-key
   ```

   Die GPG Schlüsselpaare sollten nicht von Nicht-Root-Benutzer erstellt werden. Der Root-Benutzer kann Speicherseiten sperren, was bedeutet, dass die Information nie auf Festplatte gespeichert wird, ungleich zu Nicht-Root-Benutzern.
2. Nachdem Sie den Befehl zur Generierung des Schlüsselpaares ausgeführt haben, sehen Sie einen Startbildschirm mit Schlüsseloptionen ähnlich der folgenden:

```
gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection?
```

3. Wählen Sie die Option: (2) DSA and Elgamal. Diese Option ermöglicht Ihnen, eine digitale Signatur zu erstellen und die Ver-/Entschlüsselung mit zwei verschiedenen Technologien. Geben Sie **2** ein und drücken die **Eingabe** Taste.
4. Wählen Sie als Nächstes die Schlüsselgröße aus, welche die Länge des Schlüssels festlegt. Je länger der Schlüssel, desto sicherer sind Ihre Mitteilungen gegenüber Angriffen. Wir empfehlen hierbei mindestens 2048 Bits.
5. Im Rahmen der nächsten Option werden Sie nach der Gültigkeitsdauer Ihres Schlüssels gefragt. Wenn Sie sich für ein Ablaufdatum entscheiden, dann müssen Sie auch jeden darüber informieren, der Ihren öffentlichen Schlüssel verwendet und nach Ablauf mit einem neuen Schlüssel versorgen. Es wird empfohlen, dass Sie kein Ablaufdatum eingeben. Wenn Sie kein Ablaufdatum eingeben, dann werden Sie nochmals nach einer Bestätigung gefragt:

   ```
   Key does not expire at all Is this correct (y/n)?
   ```

6. Drücken Sie **y**, um Ihre Entscheidung zu bestätigen.
7. Als Nächstes müssen Sie eine Benutzer-ID mit Ihrem Namen, Ihrer E-Mail-Adresse und einem optionalen Kommentar eingeben. Diese Informationen werden einzeln abgefragt. Wenn Sie damit fertig sind, erhalten Sie eine Zusammenfassung der von Ihnen angegebenen Informationen.
8. Geben Sie eine Passphrase ein, nachdem Sie Ihre Auswahl getroffen haben.

   Anmerkung

   Wie bei Ihren Account-Passwörtern auch, so ist eine gute Passphrase von entscheidender Bedeutung für optimale Sicherheit mit GnuPG. Ihre Passphrase sollte aus Groß- und Kleinbuchstaben, Ziffern und/oder Satzzeichen bestehen.

9. Nachdem Sie Ihre Passphrase eingegeben und bestätigt haben, werden Ihre Schlüssel generiert. Es erscheint eine Meldung ähnlich der folgenden:

   ```
   We need to generate a lot of random bytes. It is a good idea to perform some
   other action (type on the keyboard, move the mouse, utilize the disks)
   during the prime generation; this gives the random number generator a
   better chance to gain enough entropy.

   +++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++ +++.
   ++++++++++++++++++++++++++++++++++++++.........................++++
   ```

   Sobald die Aktivität auf dem Bildschirm beendet ist, werden Ihre neuen Schlüssel in das Verzeichnis **.gnupg** im Benutzerverzeichnis von Root abgelegt. Dies ist der standardmäßige Speicherort für Schlüssel, die vom Root-Benutzer erstellt werden.

Verwenden Sie folgenden Befehl, um die Schlüssel von Root anzuzeigen:

```
gpg --list-keys
```

Sie erhalten etwa folgende Ausgabe:

```
gpg: key D97D1329 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   3  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 3u
gpg: next trustdb check due at 2013-08-28
pub   2048D/D97D1329 2013-08-27 [expires: 2013-08-28]
      Key fingerprint = 29C7 2D2A 5F9B 7FF7 6411  A9E7 DE3E 5D0F D97D 1329
uid                  Your Name<you@example.com>
sub   2048g/0BE0820D 2013-08-27 [expires: 2013-08-28]
```

Um Ihren öffentlichen Schlüssel abzufragen, verwenden Sie folgenden Befehl:

```
gpg --export -a 'Your Name' > public_key.txt
```

Ihr öffentlicher Schlüssel wird in die Datei **public_key.txt** geschrieben.

Dieser öffentliche Schlüssel ist sehr wichtig. Es handelt sich nämlich dabei um den Schlüssel, der an alle Client-Systeme verteilt werden muss, die benutzerdefinierte Software via **yum** erhalten. Wie dieser Schlüssel in einer Organisation eingesetzt werden kann, wird ausführlich im *Red Hat Network Client-Konfigurationshandbuch* behandelt.

4.2.2. Pakete signieren

Bevor Sie Pakete signieren können, müssen Sie Ihre **~/.rpmmacros** Datei konfigurieren, sodass diese Folgendes beinhaltet:

```
%_signature gpg
%_gpg_name B7085C8A
```

Ersetzen Sie den **_gpg_name**-Schlüssel-ID-Wert von ***B7085C8A*** durch die Schlüssel-ID Ihres GPG-Schlüsselrings, den Sie zum Signieren von Paketen verwenden. Dieser Wert teilt **RPM** mit, welche Signatur verwendet werden soll.

Um das Paket ***package-name-1.0-1.noarch.rpm*** zu signieren, verwenden Sie folgenden Befehl:

```
rpm --resign package-name-1.0-1.noarch.rpm
```

Geben Sie Ihr Passwort ein. Um sicherzugehen, dass das Paket signiert ist, verwenden Sie folgenden Befehl:

```
rpm --checksig -v package-name-1.0-1.noarch.rpm
```

Anmerkung

Vor der Ausführung des **rpm --checksig -v** Befehls importieren Sie den GPG Schlüssel. Siehe Abschnitt 4.3, „Import benutzerdefinierte GPG-Schlüssel“ im nächsten Abschnitt für weitere Informationen.

Es sollte daraufhin Good signature from "***Your Name***" ausgegeben werden, wobei ***Your Name*** durch den Namen ersetzt wird, der mit dem jeweiligen Schlüssel verknüpft ist.

4.3. Import benutzerdefinierte GPG-Schlüssel

Allen Kunden, die ihre eigenen RPM-Dateien sicher erstellen und verteilen möchten, wird dringend empfohlen, alle angepassten RPM-Dateien mit GNU Privacy Guard (GPG) zu signieren. Das Generieren von GPG-Schlüsseln und das Erstellen von GPG-signierten Paketen wird im Abschnitt 4.2.1, „GnuPG-Schlüsselpaar generieren“ ausführlicher behandelt.

Wenn die Pakete einmal signiert sind, muss der öffentliche Schlüssel auf allen Systemen, die diese RPM-Dateien importieren, vorhanden sein. Diese Aufgabe besteht aus zwei Schritten: Zunächst muss der öffentliche Schlüssel für alle Clients zugänglich gemacht werden und im zweiten Schritt muss dann der Schlüssel dem lokalen GPG-Schlüsselring für jedes System hinzugefügt werden.

Der erste Schritt gilt für alle Systeme gleichermaßen und kann unter Verwendung des empfohlenen Website-Verfahrens zur Implementierung von Red Hat Network Client-Applikationen abgewickelt werden. Erstellen Sie hierfür ein öffentliches Verzeichnis auf dem Webserver und legen dort die öffentliche GPG-Signatur ab:

```
cp /some/path/YOUR-RPM-GPG-KEY /var/www/html/pub/
```

Der Schlüssel kann dann von Client-Systemen mittels **Wget** heruntergeladen werden:

```
wget -O- -q http://your_proxy_or_sat.your_domain.com/pub/YOUR-RPM-GPG-KEY
```

Die **-O**--Option zeigt die Resultate auf der Standardausgabe an, während die **-q**-Option **Wget** im Quiet-Modus, also ohne Bildschirmausgabe laufen lässt. Vergessen Sie nicht, die ***YOUR-RPM-GPG-KEY***-Variable durch den Dateinamen Ihres Schlüssels zu ersetzen.

Sobald der Schlüssel auf dem Client-Dateisystem vorhanden ist, importieren Sie ihn in den lokalen GPG-Schlüsselring. Unterschiedliche Betriebssysteme erfordern dazu unterschiedliche Verfahren.

Für Red Hat Enterprise Linux 3 oder höher wenden Sie folgenden Befehl an:

```
rpm --import /path/to/YOUR-RPM-GPG-KEY
```

Nachdem der GPG-Schlüssel erfolgreich dem Client hinzugefügt wurde, sollte das System in der Lage sein, benutzerdefinierte RPM-Dateien zu validieren, die mit dem dazu passenden Schlüssel signiert wurden.

Anmerkung

Wenn Sie benutzerdefinierte RPMs und Channels verwenden, erstellen Sie stets einen benutzerdefinierten GPG-Schlüssel für diese Pakete. Der Speicherort für den GPG-Schlüssel muss zudem im Kickstart-Profil eingefügt werden.
Der benutzerdefinierte GPG-Schlüssel muss zu den Client-Systemen hinzugefügt werden, andernfalls wird die Installation fehlschlagen.

Kapitel 5. Suche und Bereinigung von Fehlern

Dieses Kapitel enthält Tipps zur Suche und Bereinigung der am häufigsten auftretenden Fehler in Zusammenhang mit Red Hat Satellite. Sollten Sie zusätzliche Hilfe benötigen, dann kontaktieren Sie bitte den Red Hat Network Support unter https://access.redhat.com/support/. Melden Sie sich mit Ihrem Satellite-berechtigten Account an, um die vollständige Liste der Optionen zu erhalten.

Um mit der Problembehandlung allgemeiner Probleme zu beginnen, sehen Sie sich die Protokolldateien der Komponenten an, die das Fehlverhalten aufweisen. Nützlich ist dazu das Ausführen von **`tail -f`** für alle Protokolldateien, um danach **`yum list`** laufen zu lassen. Sie sollten anschließend alle neuen Protokolldatei-Eintragungen nach Anhaltspunkten untersuchen.

5.1. Plattenplatz

F: Mein Speicherplatz hat sich schnell gefüllt. Was ist passiert und was soll ich tun?

A: Ein häufiges Problem ist voller Festplattenspeicher. Ein nahezu sicheres Zeichen dafür ist das Auftreten von abgebrochenen Aufzeichnungen in den Protokolldateien. Wenn das Protokollieren während des Schreibvorganges abgebrochen wurde, wie beispielsweise mitten im Wort, dann sind höchstwahrscheinlich die Disks voll. Zur Bestätigung dieser Annahme führen Sie einfach folgenden Befehl aus und überprüfen die Prozentsätze in der **`Use%`** Spalte:

```
# df -h
```

Zusätzlich zu Protokolldateien können Sie auch wertvolle Informationen durch die Abfrage des Status Ihres Red Hat Satellites und dessen unterschiedlichen Komponenten erhalten. Dies erreichen Sie mithilfe des folgenden Befehls:

```
# /usr/sbin/rhn-satellite status
```

Sie können dazu auch den Status von Komponenten wie beispielsweise dem Apache Web Server und der **Red Hat Network Task Engine** individuell abfragen. Für den Apache Web Server Status führen Sie beispielsweise folgenden Befehl aus:

```
# service httpd status
```

5.2. Installieren und Aktualisieren

F: SELinux gibt laufend Meldungen aus, wenn ich zu installieren versuche. Warum?

A: Falls während der Installation von Red Hat Satellite Probleme mit SELinux-Meldungen auftreten (wie z.B. AVC Denial Meldungen), stellen Sie sicher, dass Sie die **`audit.log`** Dateien vorliegen haben, damit Ihnen der Red Hat Support behilflich sein kann. Sie finden diese Datei unter **`/var/log/audit/audit.log`** und können sie an Ihr Support-Ticket anhängen, so dass die Techniker Ihnen weiterhelfen können.

F: Ich habe `/var/satellite` in einen NFS-Mount geändert, doch SELinux verhindert jetzt, dass es korrekt funktioniert. Was muss ich tun?

A: SELinux Parameter müssen auf der Grundlage des neuen NFS-Mount geändert werden, damit SELinux diesen Datenverkehr erlaubt. Tun Sie dies mit dem folgenden Befehl:

```
# /usr/sbin/setsebool -P spacewalk_nfs_mountpoint on
```

Falls Sie Red Hat Enterprise Linux 6 verwenden, müssen Sie zudem den folgenden Befehl ausführen:

```
# /usr/sbin/setsebool -P cobbler_use_nfs on
```

F: Mein Satellite funktioniert nicht. Was könnte der Grund sein?

A: Subskribieren Sie für den Red Hat Satellite keinen der folgenden Sub-Channels, die auf den zentralen Red Hat Network Servern zur Verfügung stehen:

- Red Hat Developer Suite
- Red Hat Application Server
- Red Hat Extras
- JBoss-Produkt-Channels

Wenn Sie einen dieser Channels subskribieren und anschließend den Satellite aktualisieren, werden möglicherweise neuere, inkompatible Versionen von entscheidenden Software-Komponenten installiert, was zu einem Ausfall des Satellites führen kann.

5.3. Dienstleistungen

F: Warum läuft der Apache Web Server nicht?

A: Wenn der Apache Web Server nicht läuft, könnten Einträge in Ihrer **`/etc/hosts`** Datei fehlerhaft sein.

F: Wie finde ich den Status der Red Hat Network Task Engine heraus?

A: Um den Status der **Red Hat Network Task Engine** abzufragen, führen Sie diesen Befehl aus:

```
# service taskomatic status
```

F: Wie finde ich den Status der eingebetteten Datenbank des Satellites heraus?

A: Um den Status der eingebetteten Datenbank des Satellites abzufragen, führen Sie folgenden Befehl aus:

```
# db-control status
```

F: Was muss ich tun, wenn die Push-Funktion des Red Hat Satellites nicht mehr funktioniert?

A: Falls die push-Funktion des Red Hat Satellites plötzlich nicht mehr funktioniert, kann es sein, dass alte Protokolldateien daran schuld sind. Halten Sie den jabberd-Daemon an, bevor Sie diese Dateien entfernen. Führen Sie dazu folgende Befehle als Root aus:

```
# service jabberd stop
# rm -f /var/lib/jabberd/db/_db*
# service jabberd start
```

5.4. Verbindungsfähigkeit

F: Ich kann mich nicht verbinden! Wie kann ich feststellen, wo das Problem liegt?

A: Folgende Maßnahmen können dazu verwendet werden, allgemeine Verbindungsfehler zu finden und zu beheben:

- Versuchen Sie, in einer Befehlszeile eine Verbindung mit der Datenbank des Red Hat Satellites herzustellen, indem Sie den korrekten Verbindungsstring wie in **/etc/rhn/rhn.conf** verwenden:

```
# sqlplus username/password@sid
```

- Stellen Sie sicher, dass der Red Hat Satellite das Network Time Protocol (NTP) verwendet und auf die richtige Zeitzone eingestellt ist. Dies gilt auch für alle Client-Systeme und für den separaten Datenbankrechner bei Red Hat Satellites mit eigenständiger Datenbank.
- Bestätigen Sie das richtige Paket:

```
rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
```

  auf dem Red Hat Satellite installiert ist und dass die zugehörigen **rhn-org-trusted-ssl-cert-*.noarch.rpm** Pakete oder das öffentliche SSL-(Client)-Zertifikat der CA auf allen Client-Systemen installiert ist.
- Überprüfen Sie dass die Client-Systeme konfiguriert sind das entsprechende Zertifikat zu verwenden.
- Wenn Sie zudem einen oder mehrere Red Hat Proxy-Server verwenden, stellen Sie sicher dass alle SSL-Zertifikate des/der Proxy(s) richtig vorbereitet sind. Der Proxy sollte beides, sein eigenes Server SSL-Schlüsselpaar sowie das öffentliche SSL-(Client)-Zertifikat der CA, installiert haben, da es in beiden Eigenschaften dient. Siehe das Kapitel "SSL-Zertifikate" im *Red Hat Satellite Client Configuration Guide* für genauere Instruktionen.
- Vergewissern Sie sich, dass Client-Systeme keine eigenen Firewalls verwenden und somit erforderliche Ports blockieren, wie im *Red Hat Satellite Installation Guide*'s *Additional Requirements* Abschnitt aufgezeigt.

F: Was kann ich tun, wenn das Importieren oder Synchronisieren eines Channels fehlschlägt und ich ihn nicht wiederherstellen kann?

A: Wenn das Importieren/Synchronisieren eines Channels fehlschlägt und Sie ihn auf keine Art wiederherstellen können, führen Sie folgenden Befehl aus, um den Cache zu leeren:

```
# rm -rf temporary-directory
```

Anmerkung

Der *Red Hat Satellite Installation Guide* Abschnitt in *Preparing for Import from Local Media* spezifiziert **/var/rhn-sat-import/** als das temporäre Verzeichnis.

Starten Sie danach den Import oder die Synchronisation neu.

F: Ich erhalte "SSL_CONNECT"-Fehler. Was muss ich tun?

A: Ein häufiges Verbindungsproblem, angezeigt durch den **SSL_CONNECT** Fehler, resultiert daraus, dass ein Satellite auf einem Rechner installiert wurde, dessen Systemzeit nicht richtig eingestellt wurde. Während des Satellite-Installationsprozesses werden somit SSL-Zertifikate mit fehlerhaften Zeitangaben erstellt. Wenn die Zeit des Satellites dann korrigiert wird, kann es sein, dass das Startdatum und die festgelegte Zeit des Zertifikats in der Zukunft liegen und es daher ungültig erscheinen lassen.

Um den Fehler zu beheben, überprüfen Sie daher die Datum/Zeit-Einstellungen auf Clients und dem Satellite mit folgendem Befehl:

```
# date
```

Die Resultate sollten für alle Rechner nahezu identisch sein und innerhalb der "notBefore"- und "notAfter"-Gültigkeitsfenster des Zertifikats liegen. Überprüfen Sie die Zertifikatsdaten und -zeiten des Clients mit folgendem Befehl:

```
# openssl x509 -dates -noout -in /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

Überprüfen Sie die Daten und Zeiten des Satellite Server-Zertifikats mit folgendem Befehl:

```
# openssl x509 -dates -noout -in /etc/httpd/conf/ssl.crt/server.crt
```

Standardmäßig ist das Server-Zertifikat für ein Jahr gültig, während Client-Zertifikate für 10 Jahre gültig sind. Wenn die Zertifikate inkorrekt sind, können Sie entweder bis zur gültigen Startzeit warten oder ein neues Zertifikat erstellen. Vorzugsweise sollten alle Systemzeiten auf GMT eingestellt sein.

5.5. Protokollierung und Berichterstattung

F: Welche Protokolldateien sind relevant?

A: Nahezu jede Suche und Bereinigung von Fehlern sollte damit beginnen, sich die damit in Verbindung stehenden Protokolldateien genauer anzusehen. Diese Dateien liefern außerordentlich wertvolle Informationen über die Abläufe auf den Einheiten oder innerhalb der Applikation und können dazu verwendet werden, das allgemeine Leistungsverhalten zu überwachen und damit eine einwandfreie Konfiguration zu gewährleisten. Siehe Tabelle 5.1, „Protokolldateien“ für die Pfade zu allen relevanten Protokolldateien:

Unter Umständen sehen Sie nummerierte Protokolldateien (wie z.B. /var/log/rhn/rhn_satellite_install.log.1, /var/log/rhn/rhn_satellite_install.log.2 etc.) im **/var/log/rhn/** Verzeichnis. Dabei handelt es sich um *rotierte* Protokolldateien, die mit einer .<NUMMER>-Erweiterung erstellt werden, wenn die aktuelle **rhn_satellite_install.log** Datei bis zu einer vom **logrotate(8)** Daemon festgelegten Größe angewachsen ist, woraufhin die Inhalte in die rotierte Protokolldatei umgeschrieben werden. Beispielsweise enthält die **rhn_satellite_install.log.1** Datei die älteste rotierte Protokolldatei, während die **rhn_satellite_install.log.4** Datei die erst kürzlich rotierte Protokolldatei enthält.

Tabelle 5.1. Protokolldateien

Komponente/Aufgabe	Speicherort der Protokolldatei
Apache Web server	**`/var/log/httpd/`**-Verzeichnis
Red Hat Satellite	**`/var/log/rhn/`**-Verzeichnis
Red Hat Satellite Installationsprogramm	**`/var/log/rhn/rhn_satellite_install.log`**
Datenbankinstallation - *eingebettete Datenbank*	**`/var/log/rhn/install_db.log`**
Datenbankbelegung	**`/var/log/rhn/populate_db.log`**
Red Hat Satellite Synchronisationstool	**`/var/log/rhn/rhn_server_satellite.log`**
Monitoring-Infrastruktur	**`/var/log/nocpulse/`**-Verzeichnis
Monitoring-Benachrichtigungen	**`/var/log/notification/`**-Verzeichnis
Red Hat Network DB Control - *Eingebettete Datenbank*	**`/var/log/rhn/rhn_database.log`**
Red Hat Network Task Engine (taskomatic)	**`/var/log/messages`**
yum	**`/var/log/yum.log`**
XML-RPC-Transaktionen	**`/var/log/rhn/rhn_server_xmlrpc.log`**

F: Wie verwende ich den `spacewalk-report`-Befehl?

A: Es gibt Situationen, in denen Administratoren eine präzise, formatierte Zusammenfassung ihrer Red Hat Satellite Ressourcen benötigen, z.B. zwecks Inventur ihrer Berechtigungen, angemeldeten Systeme oder Benutzer und Organisationen. Statt diese Informationen manuell vom Satellite Interface zusammenzusuchen, beinhaltet Red Hat Satellite den **`spacewalk-report`** Befehl, der die wesentlichen Satellite-Informationen sammelt und auf einen Blick anzeigt.

Anmerkung

Um **`spacewalk-report`** zu verwenden, muss das **`spacewalk-reports`** Paket installiert sein.

`spacewalk-report` ermöglicht es Administratoren, Berichte über Inhalte, Errata, Systeme, System-Ereignischronik und Benutzerressourcen über den Satellite hinweg zu organisieren und anzuzeigen. Mithilfe von **`spacewalk-report`** erhalten Sie Berichte über:

- Systeminventar - Listet alle beim Satellite registrierten Systeme auf.
- Berechtigungen - Listet alle Organisationen auf dem Satellite auf, sortiert nach System- oder Channel-Berechtigungen.
- Errata - Listet alle Errata auf, die für die registrierten Systeme relevant sind und sortiert Errata nach Schweregrad sowie nach Systemen, auf die ein bestimmtes Erratum zutrifft.
- Benutzer - Listet alle beim Satellite registrierten Benutzer auf und führt alle mit einem bestimmten Benutzer verknüpften Systeme auf.
- Systemchronik - Listet alle oder eine Untergruppe der aufgetretenen Systemereignisse auf.

Um einen Bericht im CSV-Format zu erhalten, führen Sie den folgenden Befehl auf der Befehlszeile Ihres Satellite-Servers aus.

```
# spacewalk-report report_name
```

Die folgenden Berichte stehen zur Verfügung:

Tabelle 5.2. `spacewalk-report` Berichte

Bericht	Aufgerufen durch	Beschreibung
Systeminventar	**`inventory`**	Liste aller beim Server registrierten Systeme, zusammen mit Hardware- und Software-Informationen
Berechtigungen	**`entitlements`**	Liste aller Organisationen auf dem Satellite mit ihren System- oder Channel-Berechtigungen
Errata in Channels	**`errata-channels`**	Liste der Errata in Channels
Alle Errata	**`errata-list-all`**	Vollständige Liste aller Errata
Errata für Systeme	**`errata-systems`**	Liste zutreffender Errata sowie betroffene, registrierte Systeme
Benutzer im System	**`users`**	Liste aller beim Satellite angemeldeten Benutzer
Verwaltete Systeme	**`users-systems`**	Liste der Systeme, die durch bestimmte Benutzer verwaltet werden können
Kickstart-Bäume	**`kickstartable-trees`**	Liste aller Bäume, die gekickstartet werden können
Systemchronik	**`system-history`**	Liste der System-Ereignischronik
Systemchronik - Channels	**`system-history-channels`**	Liste der System-Ereignischronik
Systemchronik - Konfiguration	**`system-history-configuration`**	Liste der Konfigurationsereignisse des Systems
Systemchronik Berechtigungen	**`system-history-entitlements`**	Liste der Berechtigungsereignisse des Systems
Systemchronik - Errata	**`system-history-errata`**	Liste der Errata-Ereignisse des Systems
Systemchronik - Kickstart	**`system-history-kickstart`**	Liste der Kickstart- und Provisioningereignisse des Systems
Systemchronik - Pakete	**`system-history-packages`**	Liste der Paketereignisse des Systems

Führen Sie für weitere Informationen über einen bestimmten Bericht **`spacewalk-report`** mit der **`--info`** oder **`--list-fields-info`** Option und dem Berichtsnamen aus. Dies zeigt die Beschreibung sowie die Liste möglicher Felder im Bericht an.

Nutzen Sie für weitere Informationen auch die **`spacewalk-report(8)`** man-Seite sowie den **`--`**

help Parameter des **spacewalk-report** Programms, um weiterführende Informationen über die Programmaufrufe und deren Optionen zu erhalten.

F: Wie kann ich feststellen, welche Version des Datenbankschemas ich habe?

A: Um die Version des Datenbankschemas abzufragen, geben Sie folgenden Befehl ein:

```
# rhn-schema-version
```

F: Wie kann ich feststellen, welche Zeichensatztypen ich habe?

A: Um die Zeichensatztypen der Datenbank Ihres Satellites zu erhalten, führen Sie folgenden Befehl aus:

```
# rhn-charsets
```

F: Warum bekommt der Administrator keine E-Mails?

A: Wenn der Administrator keine E-Mails vom Red Hat Satellite erhält, überprüfen Sie, ob die richtige E-Mail-Adresse für **traceback_mail** in **/etc/rhn/rhn.conf** angegeben wurde.

F: Wie ändere ich den Absender der Traceback-E-Mails?

A: Wenn die Traceback-Mail mit dem Absender dev-null@rhn.redhat.com gekennzeichnet ist und Sie gerne möchten, dass diese Adresse für Ihre Organisation gültig ist, dann fügen Sie die Option **web.default_mail_from** und den entsprechenden Wert in **/etc/rhn/rhn.conf** ein.

5.6. Fehler

F: Ich erhalte während der Installation des Red Hat Satellites den Fehler "Error validating satellite certificate" (Fehler beim Validieren des Satellite-Zertifikats). Wie behebe ich dies?

A: Der Fehler "Error validating satellite certificate" (Fehler beim Validieren des Satellite-Zertifikats) während der Red Hat Satellite Installation wird durch einen HTTP-Proxy in der Umgebung verursacht. Sie können dies bestätigen, indem Sie sich die **install.log** Datei ansehen und den folgenden Fehler suchen:

```
ERROR: unhandled exception occurred:
Traceback (most recent call last):
  File "/usr/bin/rhn-satellite-activate", line 45, in ?
    sys.exit(abs(mod.main() or 0))
  File "/usr/share/rhn/satellite_tools/rhn_satellite_activate.py", line 585,
in main
    activateSatellite_remote(options)
  File "/usr/share/rhn/satellite_tools/rhn_satellite_activate.py", line 291,
in activateSatellite_remote
    ret = s.satellite.deactivate_satellite(systemid, rhn_cert)
  File "/usr/lib/python2.4/site-packages/rhn/rpclib.py", line 603, in
__call__
    return self._send(self._name, args)
  File "/usr/lib/python2.4/site-packages/rhn/rpclib.py", line 326, in _request
    self._handler, request, verbose=self._verbose)
  File "/usr/lib/python2.4/site-packages/rhn/transports.py", line 171, in
request
    headers, fd = req.send_http(host, handler)
  File "/usr/lib/python2.4/site-packages/rhn/transports.py", line 698, in
send_http
    self._connection.connect()
  File "/usr/lib/python2.4/site-packages/rhn/connections.py", line 193, in
connect
    sock.connect((self.host, self.port))
  File "<string>", line 1, in connect
socket.timeout: timed out
```

Um das Problem zu beseitigen:

1. Führen Sie das Installationsskript im Offline-Modus aus und überspringen Sie die Datenbankinstallation, die bereits erfolgt ist:

   ```
   # ./install.pl --disconnected --skip-db-install
   ```

2. Öffnen Sie die **/etc/rhn/rhn.conf** Datei in einem Texteditor Ihrer Wahl und fügen Sie die folgende Zeile hinzu bzw. ändern diese wie folgt ab:

   ```
   server.satellite.rhn_parent = satellite.rhn.redhat.com
   ```

   Entfernen Sie die folgende Zeile:

   ```
   disconnected=1
   ```

   Falls Sie einen Proxy für die Verbindung zum Red Hat Network nutzen, müssen Sie zudem die folgenden Zeilen hinzufügen bzw. ändern, um die Proxy-Einstellungen anzugeben.

   ```
   server.satellite.http_proxy = <hostname>:<port>
   server.satellite.http_proxy_username = <username>
   server.satellite.http_proxy_password = <password>
   ```

3. Reaktivieren Sie den Satellite im Online-Modus, indem Sie den Befehl **rhn-satellite-activate** als Root ausführen und den Pfad und den Dateinamen des Satellite-Zertifikats angeben:

   ```
   # rhn-satellite-activate --rhn-cert=/path/to/file.cert
   ```

Alternativ können Sie versuchen, das **install.pl**-Skript im Online-Modus auszuführen, allerdings mit der **--answer-file=*answer file*** Option. Stellen Sie sicher, dass die Antwortdatei die folgenden HTTP-Proxy-Informationen enthält:

```
rhn-http-proxy = <hostname>:<port>
rhn-http-proxy-username = <username>
rhn-http-proxy-password = <password>
```

F: Ich erhalte den Fehler "ERROR: server.mount_point not set in the configuration file" (FEHLER: server.mount_point nicht in der Konfigurationsdatei eingestellt), wenn ich den Red Hat Satellite zu aktivieren oder zu synchronisieren versuche. Wie kann ich dieses Problem beheben?

A: Der Fehler "ERROR: server.mount_point not set in the configuration file" (FEHLER: server.mount_point nicht in der Konfigurationsdatei eingestellt) beim Aktivieren oder Synchronisieren des Red Hat Satellites kann auftreten, wenn der ***mount_point*** Konfigurationsparameter in **/etc/rhn/rhn.conf** nicht auf einen Verzeichnispfad verweist, oder wenn der angegebene Verzeichnispfad nicht existiert oder darauf nicht zugegriffen werden darf.

Um das Problem zu beheben, überprüfen Sie den Wert des ***mount_point*** Konfigurationsparameters in **/etc/rhn/rhn.conf**. Ist er auf den Standardwert **/var/satellite** eingestellt, dann überprüfen Sie, ob die **/var/satellite** und **/var/satellite/redhat** Verzeichnisse existieren. Überprüfen Sie für alle Werte, dass der Pfad zur Datei fehlerfrei ist und dass die Berechtigungen korrekt gesetzt sind.

F: Warum gibt `cobbler check` einen Fehler aus, der besagt, dass er eine andere Version von `yum-utils` benötigt?

A: Gelegentlich erhalten Sie beim Ausführen des **cobbler check** Befehls einen Fehler ähnlich dem Folgenden:

```
# cobbler check
The following potential problems were detected:
#0: yum-utils need to be at least version 1.1.17 for reposync -l, current
version is 1.1.16
```

Dabei handelt es sich um ein bekanntes Problem in Cobblers **reposync** Paket. Der Fehler ist unberechtigt und kann problemlos ignoriert werden. Dieser Fehler wird in zukünftigen Versionen des Red Hat Satellites behoben werden.

F: Ich erhalte den Fehler "unsupported version" (nicht unterstützte Version), wenn ich versuche, das Red Hat Satellite Zertifikat zu aktivieren. Wie behebe ich das Problem?

A: Falls Ihr Red Hat Satellite Zertifikat beschädigt wurde, erhalten Sie ggf. einen der folgenden Fehler:

```
ERROR: <Fault -2: 'unhandled internal exception: unsupported version: 96'>
```

```
RHN_PARENT: satellite.rhn.redhat.com
     Error reported from RHN: <Fault -2: 'unhandled internal exception:
unsupported version: 115'>
     ERROR: unhandled XMLRPC fault upon remote activation: <Fault -2:
'unhandled internal exception: unsupported version: 115'>
     ERROR: <Fault -2: 'unhandled internal exception: unsupported version:
115'>
```

```
Invalid satellite certificate
```

Um dieses Problem zu beheben, setzen Sie sich bitte mit dem Red Hat Support in Verbindung, um ein neues Zertifikat zu erhalten.

F: Ich erhalte den Fehler "Internal Server Error" (Interner Server-Fehler), der sich über ASCII beschwert, wenn ich das Kickstart-Profil zu bearbeiten versuche. Wo liegt das Problem?

A: Falls Sie kürzlich einige Kernel-Parameter zu Ihrem Kickstart-Profil hinzugefügt haben, erhalten Sie unter Umständen den folgenden internen Server-Fehler, wenn Sie **`Eine Liste der Kickstart-Profile ansehen`** möchten:

```
'ascii' codec can't encode character u'\u2013'
```

Dieser Fehler tritt auf, da Teile des Textes im Profil nicht ordnungsgemäß erkannt werden können.

Um das Problem zu beseitigen:

1. Verbinden Sie sich als Root-Benutzer mittels SSH direkt mit dem Satellite Server:

   ```
   # ssh root@satellite.fqdn.com
   ```

2. Suchen Sie das Kickstart-Profil, das dieses Problem verursacht, indem Sie sich die Daten der Dateien in **`/var/lib/cobbler/config/profiles.d`** ansehen und das kürzlich geänderte Profil lokalisieren:

   ```
   # ls -l /var/lib/cobbler/config/profiles.d/
   ```

3. Öffnen Sie das Profil in einem Texteditor Ihrer Wahl und suchen Sie nach dem folgenden Text:

   ```
   \u2013hostname
   ```

   Ändern Sie diesen Eintrag auf:

   ```
   --hostname
   ```

4. Speichern Sie die Änderungen am Profil und schließen Sie die Datei.
5. Starten Sie die Red Hat Satellite Dienste neu, damit das aktualisierte Profil wirksam wird:

```
# rhn-satellite restart
Shutting down rhn-satellite...
Stopping RHN Taskomatic...
Stopped RHN Taskomatic.
Stopping cobbler daemon:                                   [  OK  ]
Stopping rhn-search...
Stopped rhn-search.
Stopping MonitoringScout ...                               [  OK  ]
Stopping Monitoring ...                                    [  OK  ]
Stopping httpd:                                            [  OK  ]
Stopping tomcat5:                                          [  OK  ]
Shutting down osa-dispatcher:                              [  OK  ]
Shutting down Oracle Net Listener ...                      [  OK  ]
Shutting down Oracle DB instance "rhnsat" ...              [  OK  ]
Shutting down Jabber router:                               [  OK  ]
Done.
Starting rhn-satellite...
Starting Jabber services                                   [  OK  ]
Starting Oracle Net Listener ...                           [  OK  ]
Starting Oracle DB instance "rhnsat" ...                   [  OK  ]
Starting osa-dispatcher:                                   [  OK  ]
Starting tomcat5:                                          [  OK  ]
Starting httpd:                                            [  OK  ]
Starting Monitoring ...                                    [  OK  ]
Starting MonitoringScout ...                               [  OK  ]
Starting rhn-search...
Starting cobbler daemon:                                   [  OK  ]
Starting RHN Taskomatic...
Done.
```

6. Gehen Sie zurück zur Weboberfläche. Beachten Sie, dass die Weboberfläche ggf. einige Zeit benötigt, um die Dienste aufzulösen. Es sollte nach einiger Zeit auf normal zurückkehren.

F: Ich erhalte den Fehler "Host Not Found" (Host nicht gefunden) oder "Could Not Determine FQDN" (FQDN konnte nicht ermittelt werden). Was sollte ich deshalb unternehmen?

A: Da Red Hat Network Konfigurations-Dateien ausschließlich auf voll qualifizierte Domain-Namen (FQDNs) angewiesen sind, ist es unerlässlich, dass Schlüsselapplikationen den Namen des Red Hat Satellites in eine IP-Adresse auflösen können. **Red Hat Update Agent**, **Red Hat Network Registration Client** und der Apache Web Server sind für dieses Problem besonders anfällig, wodurch die Red Hat Network Applikationen Fehlermeldungen wie "host not found" (Host nicht gefunden) ausgeben und der Web-Server "Could not determine the server's fully qualified domain name" (FQDN konnte nicht ermittelt werden) angibt, nachdem er nicht starten konnte.

Dieses Problem hat normalerweise seine Ursache in der **`/etc/hosts`** Datei. Sie können diese Annahme bestätigen, indem Sie sich die Datei **`/etc/nsswitch.conf`** genauer ansehen, in der das Verfahren und die Reihenfolge festgelegt wird, in der Domainnamen aufgelöst werden. Normalerweise wird die Datei **`/etc/hosts`** zuerst überprüft, gefolgt vom Network Information Service (NIS), gefolgt von DNS. Eine dieser Überprüfungen muss erfolgreich sein, damit der Apache Web Server starten kann und die Red Hat Network Client-Applikationen funktionieren können.

Um dieses Problem zu beheben, sehen Sie sich die Inhalte der **`/etc/hosts`** Datei genauer an. Diese können ungefähr so aussehen:

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain \
localhost
```

Entfernen Sie zunächst in einem Texteditor die entsprechende Rechnerinformation. Gehen Sie dazu folgendermaßen vor:

```
127.0.0.1 localhost.localdomain.com localhost
```

Speichern Sie daraufhin die Datei und versuchen Sie die Red Hat Network Client-Applikationen nochmals auszuführen oder den Apache Web Server zu starten. Wenn dies immer noch fehlschlägt, dann geben Sie ausdrücklich die IP-Adresse des Proxys in der Datei an, wie z.B.:

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Ersetzen Sie hier den Wert mit der tatsächlichen IP-Adresse des Satellites. Damit sollte das Problem behoben sein. Denken Sie daran, falls die IP-Adresse auf diese Art festgelegt ist, muss diese Datei immer dann aktualisiert werden, wenn der Rechner eine neue Adresse erhält.

F: Ich erhalte den Fehler "This server is not an entitled Satellite" (Dieser Server ist kein berechtigter Satellite), wenn ich mit dem Red Hat Satellite Server zu synchronisieren versuche. Wie behebe ich dieses Problem?

A: Falls **`satellite-sync`** meldet, dass der Server nicht als ein Red Hat Satellite aktiviert ist, dann ist er nicht bei dem jeweiligen Red Hat Satellite Channel angemeldet. Falls es sich um ein neu installiertes System handelt stellen Sie sicher dass das Satellite-Zertifikat auf dem System aktiviert ist. Falls es früher bereits aktiviert war, wurde es in der Zwischenzeit deaktiviert.

Überprüfen Sie die Sub-Channels des Systems, um festzustellen, ob es bei Red Hat Network Red Hat Satellite Channels angemeldet ist. Anzeigen der subskribierten Channels mit dem folgenden Befehl:

```
# yum repolist
```

Aktivieren Sie dasselbe Satellite-Zertifikat erneut auf Ihrem Satellite, indem Sie den folgenden Befehl als Root ausführen:

```
# rhn-satellite-activate -vvv --rhn-cert=/path/to/certificate
```

5.7. Weboberfläche

F: Ich habe Probleme mit der Red Hat Satellite Benutzeroberfläche. Welche Protokolldateien sollte ich überprüfen?

A: Falls Sie in der Red Hat Satellite Benutzeroberfläche beim Anzeigen, Einplanen oder Arbeiten mit Kickstarts Probleme haben, überprüfen Sie die **`/var/log/tomcat6/catalina.out`** Protokolldatei.

Für alle anderen Probleme mit der Benutzeroberfläche werfen Sie bitte einen Blick auf die **`/var/log/httpd/error_log`**-Protokolldatei.

5.8. Anaconda

F: Ich erhalte den Fehler "`Error downloading kickstart file`" (Fehler beim Herunterladen der Kickstart-Datei). Wo liegt das Problem und wie behebe ich es?

A: Dieser Fehler wird meist durch ein Problem mit der Netzwerkverbindung verursacht. Um das Problem ausfindig zu machen, führen Sie den Befehl **`cobbler check`** aus und lesen Sie sich dessen Ausgabe durch, die etwa folgendermaßen aussehen sollte:

```
# cobbler check
The following potential problems were detected:
#0: reposync is not installed, need for cobbler reposync, install/upgrade
yum-utils?
#1: yumdownloader is not installed, needed for cobbler repo add with --rpm-
list parameter, install/upgrade yum-utils?
#2: The default password used by the sample templates for newly installed
machines (default_password_crypted in /etc/cobbler/settings) is still set to
'cobbler' and should be changed
#3: fencing tools were not found, and are required to use the (optional) power
management features. install cman to use them
```

Falls **`cobbler check`** keine Antworten liefert, überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass **`httpd`** läuft: **`service httpd status`**
- Vergewissern Sie sich, dass **`cobblerd`** läuft: **`service cobblerd status`**
- Vergewissern Sie sich, dass Sie die Kickstart-Datei mittels **`wget`** von einem anderen Host aus abrufen können:

```
wget http://satellite.example.com/cblr/svc/op/ks/profile/rhel5-i386-
u3:1:Example-Org
```

F: Ich erhalte bei der Paketinstallation den Fehler "`The file chkconfig-1.3.30.1-2.i386.rpm cannot be opened.`" (Die Datei chkconfig-1.3.30.1-2.i386.rpm konnte nicht geöffnet werden). Wo liegt das Problem und wie behebe ich es?

A: Clients beziehen Inhalte vom Red Hat Satellite basierend auf dem ***`--url`*** Parameter innerhalb des Kickstarts. Zum Beispiel:

```
url --url http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-u3
```

Falls Sie Fehlermeldungen von Anaconda erhalten, die besagen, dass es keine Images oder Pakete finden kann, sollten Sie überprüfen, ob die obige URL eine ***`200 OK`*** Antwort generiert. Versuchen Sie dazu, die Datei unter der URL mittels **`wget`** abzurufen:

```
wget http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-u3
--2011-08-19 15:06:55--  http://satellite.example.com/ks/dist/ks-rhel-i386-
server-5-u3
Resolving satellite.example.com... 10.10.77.131
Connecting to satellite.example.com|10.10.77.131|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]
Saving to: `ks-rhel-i386-server-5-u3.1'
2011-08-19 15:06:55 (0.00 B/s) - `ks-rhel-i386-server-5-u3.1' saved [0/0]
```

Wenn Sie keine ***`200 OK`*** Antwort erhalten, überprüfen Sie die Fehlerprotokolle, um herauszufinden,

wo der Fehler liegt. Sie können auch die Datei selbst überprüfen, die Anaconda herunterzuladen versuchte, indem Sie die **access_log** Datei durchsuchen:

```
# grep chkconfig /var/log/httpd/access_log
10.10.77.131 - - [19/Aug/2011:15:12:36 -0400] "GET
/rhn/common/DownloadFile.do?url=/ks/dist/ks-rhel-i386-server-
5-u3/Server  /chkconfig-1.3.30.1-2.i386.rpm HTTP/1.1" 206 24744 "-"
"urlgrabber/3.1.0 yum/3.2.19"
10.10.76.143 - - [19/Aug/2011:15:12:36 -0400] "GET /ks/dist/ks-rhel-i386-
server-5-u3/Server/chkconfig-
1.3.30.1-2.i386.rpm HTTP/1.1" 206 24744 "-" "urlgrabber/3.1.0 yum/3.2.19"
10.10.76.143 - - [19/Aug/2011:15:14:20 -0400] "GET /ks/dist/ks-rhel-i386-
server-5-u3/Server/chkconfig-
1.3.30.1-2.i386.rpm HTTP/1.1" 200 162580 "-" "urlgrabber/3.1.0 yum/3.2.19"
10.10.77.131 - - [19/Aug/2011:15:14:20 -0400] "GET
/rhn/common/DownloadFile.do?url=/ks/dist/ks-rhel-i386-server-
5-u3/Server/chkconfig-1.3.30.1-2.i386.rpm HTTP/1.1" 200 162580 "-"
"urlgrabber/3.1.0 yum/3.2.19"
```

Falls diese Anfragen nicht in der **access_log** Datei erscheinen, liegt ggf. ein Problem mit den Netzwerkeinstellungen des Systems vor. Falls die Anfragen erscheinen, jedoch Fehler generieren, überprüfen Sie die Fehlerprotokolle.

Sie können auch versuchen, die Dateien manuell herunterzuladen, um festzustellen, ob das Paket verfügbar ist:

```
wget http://satellite.example.com/ks/dist/ks-rhel-i386-server-5-
u3/Server/chkconfig-1.3.30.1-2.i386.rpm
```

5.9. Tracebacks

F: Ich bekomme E-Mails mit dem Betreff "WEB TRACEBACK". Was sollte ich deshalb unternehmen?

A: Eine typische Traceback-E-Mail sieht etwa folgendermaßen aus:

```
Subject: WEB TRACEBACK from satellite.example.com
Date: Wed, 19 Aug 2011 20:28:01 -0400
From:Red Hat Satellite <dev-null@redhat.com>
To: admin@example.com

java.lang.RuntimeException: XmlRpcException calling cobbler.
 at
com.redhat.rhn.manager.kickstart.cobbler.CobblerXMLRPCHelper.invokeMethod(Cobb
lerXMLRPCHelper.java:72)
 at
com.redhat.rhn.taskomatic.task.CobblerSyncTask.execute(CobblerSyncTask.java:76)
 at
com.redhat.rhn.taskomatic.task.SingleThreadedTestableTask.execute(SingleThreaded
TestableTask.java:54)
 at org.quartz.core.JobRunShell.run(JobRunShell.java:203)
 at
org.quartz.simpl.SimpleThreadPool$WorkerThread.run(SimpleThreadPool.java:520)
Caused by: redstone.xmlrpc.XmlRpcException: The response could not be parsed.
 at redstone.xmlrpc.XmlRpcClient.handleResponse(XmlRpcClient.java:434)
 at redstone.xmlrpc.XmlRpcClient.endCall(XmlRpcClient.java:376)
 at redstone.xmlrpc.XmlRpcClient.invoke(XmlRpcClient.java:165)
 at
com.redhat.rhn.manager.kickstart.cobbler.CobblerXMLRPCHelper.invokeMethod(Cobb
lerXMLRPCHelper.java:69)
 ... 4 more
Caused by: java.io.IOException: Server returned HTTP response code: 503 for
URL: http://someserver.example.com:80/cobbler_api
 at
sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.jav
a:1236)
 at redstone.xmlrpc.XmlRpcClient.handleResponse(XmlRpcClient.java:420)
 ... 7 more
```

Dies zeigt an, dass bei der Kommunikation von Cobbler mit dem **taskomatic** Dienst ein Problem auftrat. Überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass **httpd** läuft: **# service httpd status**
- Vergewissern Sie sich, dass **cobblerd** läuft: **# service cobblerd status**
- Vergewissern Sie sich, dass es keine Firewall-Regeln gibt, die **localhost** Verbindungen verhindern

5.10. Registrierung

F: Der rhnreg_ks Befehl schlägt fehl mit der Meldung "ERROR: unable to read system id" (Fehler: System-ID konnte nicht gelesen werden). Wo liegt das Problem?

A: Am Ende der Kickstart-Datei gibt es einen **%post** Abschnitt, der den Rechner beim Red Hat Satellite registriert:

```
# begin Red Hat management server registration
mkdir -p /usr/share/rhn/
wget http://satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT -O
/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
perl -npe 's/RHNS-CA-CERT/RHN-ORG-TRUSTED-SSL-CERT/g' -i /etc/sysconfig/rhn/*
rhnreg_ks --serverUrl=https://satellite.example.com/XMLRPC --
sslCACert=/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT --activationkey=1-
c8d01e2f23c6bbaedd0f6507e9ac079d
# end Red Hat management server registration
```

Dadurch werden folgende Aktionen in der angegebenen Reihenfolge ausgeführt:

- Erstellen eines Verzeichnisses für das benutzerdefinierte SSL-Zertifikat, das vom Red Hat Satellite verwendet wird.
- Abrufen des SSL-Zertifikats, das während der Registrierung verwendet wird.
- Suchen und ersetzen Sie die SSL-Zertifikat Strings in der **`rhn-register`** Konfigurationsdatei und registrieren Sie unter Verwendung des SSL-Zertifikats und eines Aktivierungsschlüssels beim Red Hat Satellite. Jedes Kickstart-Profil enthält einen Aktivierungsschlüssel, der sicherstellt, dass dem System die richtigen Basis- und Sub-Channels zugewiesen werden und es die richtigen Systemberechtigungen erhält. Falls es sich um Reprovisioning eines vorhandenen Systems handelt, wird der Aktivierungsschlüssel auch sicherstellen, dass es wieder mit dem früheren Systemprofil verknüpft wird.

Falls der **`rhnreg_ks`** Befehl fehlschlägt, sehen Sie ggf. folgende Fehlermeldungen in der **`ks-post.log`** Datei:

```
ERROR: unable to read system id.
```

Diese Fehler treten auch dann auf, wenn Sie versuchen, einen **`rhn_check`** durchzuführen, das System jedoch nicht beim Red Hat Satellite registriert wurde.

Sehen Sie sich zur Suche und Bereinigung dieses Fehlers am besten die Kickstart-Datei an und kopieren die oben genannten vier Schritte in eine Eingabeaufforderung und führen diese aus, nachdem der Kickstart abgeschlossen wurde. Dadurch werden detailliertere Fehlermeldungen generiert, die Ihnen bei der Suche nach der Ursache des Problems helfen können.

5.11. Kickstarts und Snippets

F: Wie sieht die Verzeichnisstruktur für Kickstarts aus?

A: Der Basispfad, unter dem Kickstart-Dateien gespeichert werden, ist **`/var/lib/rhn/kickstarts/`**. In diesem Verzeichnis befinden sich Raw-Kickstarts in dem Unterverzeichnis **`upload`**, während sich die per Assistent generierten Kickstarts in dem Unterverzeichnis **`wizard`** befinden:

```
Raw-Kickstarts: /var/lib/rhn/kickstarts/upload/$profile_name--$org_id.cfg
Assistenten-Kickstarts: /var/lib/rhn/kickstarts/wizard/$profile_name--
$org_id.cfg
```

F: Wie sieht die Verzeichnisstruktur für Cobbler-Snippets aus?

A: Cobbler-Snippets werden unter **`/var/lib/rhn/kickstarts/snippets`** gespeichert. Cobbler greift über den symbolischen Link **`/var/lib/cobbler/snippets/spacewalk`** auf die Snippets

zu.

```
Snippets:  /var/lib/rhn/kickstarts/snippets/$org_id/$snippet_name
```

Wichtig

Red Hat Satellite RPMs erwarten die Cobbler-Kickstart und Snippet-Verzeichnisse an ihren standardmäßigen Speicherorten, ändern Sie diese also nicht.

5.12. Monitoring

F: Gibt es irgendwelche Diagnose-Tools, welche bei der Ermittlung der Ursache für die Überwachungs-Fehler helfen?

A: Obwohl sämtliche Monitoring-bezogene Aktivitäten über die Satellite Interface durchgeführt werden, bietet Red Hat Zugang zu einigen Befehlszeilen-Diagnosetools, welche Ihnen beim Ermitteln von Fehlerquellen behilflich sein könnten. Um diese Tools zu benutzen, müssen Sie in der Lage sein, **nocpulse** Benutzer auf dem Satellite zu werden, der die Überwachung durchführt.

Melden Sie sich zunächst im Satellite als Root an. Wechseln Sie dann zum **nocpulse** Benutzer, indem Sie folgenden Befehl ausführen:

```
su - nocpulse
```

Zur gründlichen Beseitigung von Problemen einer Probe müssen Sie zunächst dessen Probe-ID ausfindig machen. Führen Sie dazu den Befehl **rhn-catalog** auf dem Red Hat Satellite Server als der **nocpulse** Benutzer aus. Die Ausgabe sieht etwa wie folgt aus:

```
2 ServiceProbe on example1.redhat.com (199.168.36.245): test 2
3 ServiceProbe on example2.redhat.com (199.168.36.173): rhel2.1 test
4 ServiceProbe on example3.redhat.com (199.168.36.174): SSH
5 ServiceProbe on example4.redhat.com (199.168.36.175): HTTP
```

Die Probe-ID ist die erste Zahl in der Zeile, wogegen der Probe-Name (wie auf dem Satellite Interface eingegeben) der letzte Eintrag auf der Zeile ist. Beispielsweise entspricht die Probe-ID 5 der Probe mit dem Namen HTTP.

Die Optionen **--commandline** (**-c**) und **--dump** (**-d**) gemeinsam mit der Probe-ID und **rhn-catalog** ermöglichen es Ihnen, zusätzliche Details über die Probe zu erhalten:

```
rhn-catalog --commandline --dump 5
```

Die Option **--commandline** liefert die gesetzten Befehls-Parameter für die Probe, wogegen **--dump** alle anderen Informationen einholt, inklusive Alarm-Grenzwerte sowie Benachrichtigungs-Intervalle und -Methoden.

Der oben gezeigte Befehl hat eine Ausgabe ähnlich wie diese zur Folge:

```
5 ServiceProbe on example4.redhat.com (199.168.36.175  ):
linux:cpu usage
      Run as: Unix::CPU.pm --critical=90 --sshhost=199.168.36.175
--warn=70 --timeout=15 --sshuser=nocpulse
--shell=SSHRemoteCommandShell --sshport=4545
```

Da Sie nun die ID kennen, können Sie diese mit **rhn-runprobe** verwenden, um die Ausgabe der Probe zu untersuchen.

F: Wie interpretiere ich die Ausgabe von rhn-runprobe?

A: Da Sie nun die Probe-ID mittels **rhn-catalog** erhalten haben, können Sie diese in Verbindung mit **rhn-runprobe** verwenden, um die gesamte Ausgabe der Probe zu untersuchen. Beachten Sie, dass standardmäßig **rhn-runprobe** im Testmodus abläuft, was bedeutet, dass keine Ergebnisse in die Datenbank eingegeben werden. Hier finden Sie einige Optionen:

Tabelle 5.3. rhn-runprobe-Optionen

Option	Beschreibung
--help	Listet die verfügbaren Optionen auf und beendet.
--probe=*PROBE_ID*	Führt die Probe mit dieser ID aus.
--prob_arg=*PARAMETER*	Setzt jegliche Probe-Parameter aus der Datenbank außer Kraft.
--module=*PERL_MODULE*	Paketname von alternativem auszuführendem Code.
--log=all=*LEVEL*	Setzt die Protokollierungsebene für ein Paket oder Paket-Präfix.
--debug=*LEVEL*	Setzt numerischen Debugging-Level.
--live	Führt die Probe aus, reiht Daten ein und sendet Benachrichtigungen aus (falls erforderlich).

Sie sollten mindestens die **--probe**- und die **--log** Option sowie die jeweiligen Werte einfügen. Die **--probe** Option akzeptiert die Probe-ID als Wert und die **--log** Option akzeptiert den Wert "all" (für alle Runlevel) und eine numerischen Verbositäts-Ebene als Werte. Hier ist ein Beispiel:

```
rhn-runprobe --probe=5 --log=all=4
```

Der oben angeführte Befehl fordert die Probe-Ausgabe für probeID 5 an, für alle Runlevel und mit einem hohen Grad an Verbosität (Ausführlichkeit der Ausgabe).

Sie können auch die aus **rhn-catalog** abgeleiteten Befehls-Parameter verwenden, wie z.B.:

```
rhn-runprobe 5 --log=all=4 --sshuser=nocpulse --sshport=4545
```

Dies hat eine sehr ausführliche Ausgabe zur Folge, die den Ausführungsversuch der Probe schildert. Fehler werden dabei klar ersichtlich.

5.13. Mehrfach-Organisationen Satellites und Satellite Zertifikate

F: Wie registriere ich meine Systeme in einer Mehrfach-Organisationen Umwelt, wenn ich nicht genügend Berechtigungen in meinem Satelliten-Zertifikat habe?

A: Es können Situationen auftreten, in denen Sie Berechtigungen frei machen müssen, aber wenig

Zeit zur Verfügung haben sowie evtl. keinen Zugang zu jeder Organisation besitzen, um dies selbst zu erledigen. Es gibt eine Option in Mehrfach-Organisationen-Satellites, die es dem Systemadministrator erlaubt, die Anzahl von Berechtigungen einer Organisation unter den tatsächlichen Gebrauch zu senken. Dieses Verfahren muss angemeldet bei der administrativen Organisation durchgeführt werden.

Wenn Sie bei der administrativen Organisation angemeldet sind und Ihr Zertifikat beispielsweise 5 System-Management-Berechtigungen zu wenig besitzt, um alle auf Ihrem Satellite registrierten Systeme abzudecken, dann werden den 5 zuletzt für diese Organisation registrierten Systeme die Berechtigungen entzogen. Dieser Prozess wird nachfolgend erläutert:

1. Setzen Sie in der **`/etc/rhn/rhn.conf`** Datei ***`web.force_unentitlement`*** auf 1.
2. Starten Sie den Satellite neu.
3. Verringern Sie die zugewiesenen Berechtigungen für die gewünschten Organisationen entweder über den **`Subskriptionen`** Tab jeder Organisation, oder über die **`Organisationen`** Tabs der einzelnen Berechtigungen.
4. Eine Anzahl von Systemen in der Organisation sollte sich nun in einem **`unberechtigt`** Zustand befinden. Die Anzahl der unberechtigten Systeme in der Organisation entspricht der Differenz zwischen der Gesamtanzahl der von Ihnen der Organisation entzogenen Berechtigungen und der Anzahl von Berechtigungen, die die Organisation nicht auf die Systeme angewendet hatte.

   Wenn Sie z.B. in Schritt 3 der Organisation 10 Berechtigungen entzogen haben, und die Organisation 4 Berechtigungen besitzt, die nicht von Systemen verwendet wurden, dann werden letztendlich 6 Systeme in dieser Organisation unberechtigt sein.

Nachdem Sie die erforderliche Anzahl von Berechtigungen haben, sollte es Ihnen nun möglich sein, Ihr neues Satellite-Zertifikat zu aktivieren. Beachten Sie, dass ein Modifizieren der ***`web.force_unentitlement`*** Variablen nur nötig ist, um die einer Organisation zugewiesenen Berechtigungen unter die Anzahl der verwendeten zu verringern. Wenn eine Organisation mehr Berechtigungen besitzt, als aktiv verwendet werden, brauchen Sie diese Variable nicht zu setzen, um sie zu entziehen.

F: Ich habe zusätzliche Berechtigungen auf meinem Satellite-Zertifikat, die nicht verwendet werden. Was passiert mit diesen Berechtigungen?

A: Falls Ihnen ein neues Satellite-Zertifikat ausgestellt wird, welches mehr Berechtigungen enthält, als auf Ihrem Satellite verbraucht werden, werden jegliche überzähligen Berechtigungen der administrativen Organisation zugewiesen. Wenn Sie sich auf der Weboberfläche als Satellite-Administrator anmelden, können Sie diese Berechtigungen anderen Organisationen zuweisen. Die zuvor zu einer Organisation zugewiesenen Berechtigungen werden hiervon nicht berührt.

5.14. Proxy Installation und Konfiguration

F: Wie kann ich nach der Konfiguration des Red Hat Network Package Managers feststellen, ob die lokalen Pakete erfolgreich zum privaten Red Hat Network Channel hinzugefügt wurden?

A: Führen Sie den Befehl **`rhn_package_manager -l -c "name_of_private_channel"`** aus, um die dem Satellite bekannten Pakete in den privaten Channels aufzulisten. Oder verwenden Sie dazu das Satellite Interface.

Nachdem Sie ein registriertes System bei einem privaten Channel subskribiert haben, können Sie auch den **`yum --disablerepo="*" --enablerepo="your_repo_name" list`**

`available` Befehl auf den registrierten Systemen anwenden, um im privaten Satellite Channel nach den Paketen zu suchen.

F: Wie kann ich feststellen, ob die Clients mit dem Squid-Server verbunden sind?

A: Die **`/var/log/squid/access.log`** Datei protokolliert alle Verbindungen zum Squid-Server.

F: Der Red Hat Update Agent auf dem Client-System verbindet nicht über den Red Hat Satellite Proxy. Wie kann dieser Fehler behoben werden?

A: Vergewissern Sie sich, dass die neueste Version des Red Hat Update Agents auf den Client-Systemen installiert ist. Die neuste Version enthält die Features, die zur Verbindung durch einen Red Hat Satellite Proxy notwendig sind. Die neueste Version erhalten Sie über das Red Hat Network durch Ausführen des **`yum update yum`** Befehls als Root oder von http://www.redhat.com/support/errata/.

Der Red Hat Satellite Proxy ist eine Erweiterung von Apache. Siehe den *Log Files* Abschnitt des *Red Hat Satellite Proxy Installation Guide* für die Lage der Protokolldatei.

F: Meine Red Hat Satellite Proxy Konfiguration funktioniert nicht. Wo fange ich mit der Fehlersuche an?

A: Überprüfen Sie, ob **`/etc/sysconfig/rhn/systemid`** dem Benutzer root.apache gehört und die Berechtigungen 0640 besitzt.

Lesen Sie die Log-Dateien. Eine Liste finden Sie im *Log Files* Abschnitt des *Red Hat Satellite Proxy Installation Guide*.

F: Wie kann ich generelle Probleme in der Red Hat Satellite Proxy beheben?

A: Um mit der Behandlung von allgemeinen Problemen zu beginnen, untersuchen Sie die Protokolldatei(en), die mit der Komponente in Zusammenhang stehen, die das Fehlverhalten aufweist.

Ein häufiges Problem ist voller Festplattenspeicher. Ein nahezu sicheres Zeichen dafür ist das Auftreten von abgebrochenen Aufzeichnungen in den Protokolldateien. Wenn das Protokollieren während des Schreibvorganges abgebrochen wurde, wie beispielsweise mitten im Wort, dann sind höchstwahrscheinlich die Disks voll. Zur Bestätigung dieser Annahme führen Sie einfach folgenden Befehl aus und überprüfen die Prozentsätze in der Use% Spalte:

```
df -h
```

Zusätzlich zu Protokolldateien können Sie wertvolle Information auch durch die Abfrage des Status Ihrer unterschiedlichen Komponenten erhalten. Dies ist für den Apache Web Server und Squid möglich.

Um den Apache Web Server Status abzufragen, führen Sie den folgenden Befehl aus:

```
service httpd status
```

Um den Squid-Status abzufragen, führen Sie den folgenden Befehl aus:

```
service squid status
```

Wenn der Administrator keine E-Mails vom Red Hat Satellite Proxy erhält, überprüfen Sie, ob die richtige E-Mail-Adresse für **traceback_mail** in **/etc/rhn/rhn.conf** angegeben wurde.

F: Mein Red Hat Satellite Proxy hat den Fehler "Host Not Found"/"Could not Determine FQDN ("Host nicht gefunden"/"FQDN konnte nicht ermittelt werden") vorgefunden. Was soll ich tun?

A: Da die Red Hat Network Konfigurations-Dateien ausschließlich auf voll qualifizierte Domain-Namen (FQDNs) angewiesen sind, ist es unerlässlich, dass Schlüsselapplikationen den Namen des Red Hat Satellites in eine IP-Adresse auflösen können. Red Hat Update Agent, Red Hat Network Registration Client und der Apache Web Server sind für dieses Problem besonders anfällig, wodurch die Red Hat Network Applikationen Fehlermeldungen wie "host not found" (Host nicht gefunden) ausgeben und der Web-Server "Could not determine the server's fully qualified domain name" (FQDN konnte nicht ermittelt werden) angibt, nachdem er nicht starten konnte.

Dieses Problem hat seine Ursache in der **/etc/hosts** Datei. Sie können diese Annahme bestätigen, indem Sie sich die Datei **/etc/nsswitch.conf** genauer ansehen, in der das Verfahren und die Reihenfolge festgelegt wird, in der Domainnamen aufgelöst werden. Normalerweise wird die Datei **/etc/hosts** zuerst überprüft, gefolgt vom Network Information Service (NIS), gefolgt von DNS. Eine dieser Überprüfungen muss erfolgreich sein, damit der Apache Web Server starten kann und die Red Hat Network Client-Applikationen funktionieren können.

Um dieses Problem zu beheben, sehen Sie sich die Inhalte der **/etc/hosts** Datei genauer an. Diese können ungefähr so aussehen:

```
127.0.0.1 this_machine.example.com this_machine localhost.localdomain \
localhost
```

In einem Text-Editor entfernen Sie die Maschinen Host-Informationen aus der Datei. Es sollte so aussehen:

```
127.0.0.1 localhost.localdomain.com localhost
```

Speichern Sie die Datei und versuchen Sie die Red Hat Network Client-Applikationen nochmals auszuführen oder den Apache Web Server zu starten. Wenn dies immer noch fehlschlägt, dann geben Sie ausdrücklich die IP-Adresse des Proxys in der Datei an, wie z.B.:

```
127.0.0.1 localhost.localdomain.com localhost
123.45.67.8 this_machine.example.com this_machine
```

Ersetzen Sie hier den Wert durch die tatsächliche IP-Adresse des Proxys. Damit sollte das Problem behoben sein. Denken Sie daran dass, falls diese spezielle IP-Adresse auf diese Art festgelegt ist, die Datei immer dann aktualisiert werden muss, wenn die Maschine eine neue Adresse erhält.

F: Ich habe Probleme mit dem Red Hat Satellite Proxy und Netzwerkverbindungs-Fehler. Was soll ich tun?

A: Wenn Sie Probleme haben, die wahrscheinlich auf eine fehlgeschlagene Verbindung

zurückzuführen sind, dann können Sie Folgendes tun:

- Bestätigen Sie das richtige Paket:

  ```
  rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm
  ```

  auf dem Red Hat Satellite Proxy installiert ist und dass die zugehörigen **rhn-org-trusted-ssl-cert-*.noarch.rpm** Pakete oder das öffentliche SSL-(Client)-Zertifikat der CA auf allen Client-Systemen installiert ist.
- Überprüfen Sie dass die Client-Systeme konfiguriert sind das entsprechende Zertifikat zu verwenden.
- Wenn Sie einen oder mehrere Red Hat Satellite Proxies verwenden, überprüfen Sie, ob das SSL-Zertifikat eines jeden Proxys richtig vorbereitet ist. Wenn Sie den Red Hat Satellite Proxy in Verbindung mit einem Red Hat Satellite verwenden, sollte der Proxy sowohl sein eigenes Server-SSL-Schlüsselpaar als auch das öffentliche SSL-(Client)-Zertifikat Ihrer CA installiert haben. Für detaillierte Informationen verweisen wir dazu auf das Kapitel SSL-Zertifikate im *Red Hat Satellite Client-Konfigurationshandbuch*.
- Falls der Red Hat Satellite Proxy über ein HTTP-Proxy verbindet, überprüfen Sie, ob die URL gültig ist. Beispielsweise sollte das HTTP-Proxy URL-Feld keine Verweise auf Protokolle enthalten, wie beispielsweise http:// oder https://. Nur der Hostname und Port sollten als hostname:port, wie beispielsweise **your-gateway.example.com:8080**, angegeben werden.
- Vergewissern Sie sich, dass Client-Systeme keine eigenen Firewalls verwenden und somit erforderliche Ports blockieren, wie im *Additional Requirements* Abschnitt des *Red Hat Satellite Proxy Installation Guide* aufgezeigt.

F: Ich habe Probleme mit Paket Zustellungs-Fehlern und Objekt Korruption. Was soll ich prüfen?

A: Falls die Paketlieferung fehlschlägt oder ein Objekt fehlerhaft erscheint und dies nicht auf Verbindungsfehler zurückzuführen ist, sollten Sie in Betracht ziehen, die Caches zu leeren. Der Red Hat Satellite Proxy besitzt zwei Caches, mit denen Sie sich befassen sollten: einen für Squid und den anderen zur Authentifizierung.

Der Squid-Cache befindet sich in **/var/spool/squid/**. Um ihn zu löschen:

1. Anhalten des Apache Web Servers: **service httpd stop**
2. Anhalten des Squid Servers: **service squid stop**
3. Löschen Sie den Inhalt des Verzeichnisses: **rm -fv /var/cache/rhn/***
4. Starten Sie beide Dienste neu:

   ```
   service squid start
   service httpd start
   ```

Die gleiche Aufgabe kann schneller durch Löschen des Verzeichnisses und Neustart von Squid erreicht werden, aber diese Methode wird höchstwahrscheinlich zu einer Anzahl von Red Hat Network Traceback-Nachrichten führen.

Der interne Caching-Mechanismus, der durch das Proxy zur Authentifizierung verwendet wird, sollte eventuell ebenfalls entleert werden. Führen Sie dazu den folgenden Befehl aus:

```
rm -fv /var/cache/rhn/*
```

Anmerkung

Wenn Sie alle diese Schritte zur Suche und Bereinigung von Fehlern ausgeschöpft haben oder den Red Hat Network Experten den Vortritt lassen möchten, empfiehlt Ihnen Red Hat, dass Sie die Vorteile des Support-Services nutzen, der den Red Hat Satellite begleitet. Dabei ist es am effizientesten, die Konfigurationsparameter, Protokolldateien und Datenbankinformationen Ihres Satellites zusammenzufassen und gebündelt direkt an Red Hat zu senden.
Red Hat Network stellt ein Befehlszeilen-Tool explizit für diesen Zweck zur Verfügung: Den sogenannten **Satellite Diagnostic Info Gatherer**, für gewöhnlich auch nach dessen Befehl **`satellite-debug`** benannt. Um dieses Tool zu verwenden, führen Sie einfach diesen Befehl als Root aus. Sie sehen dabei die einzelnen Teile an Information, die gesammelt werden, in einem einzigen erzeugten Tarball, z.B.:

```
# satellite-debug
Collecting and packaging relevant diagnostic information.
Warning: this may take some time...
    * copying configuration information
    * copying logs
    * querying RPM database (versioning of Red Hat Satellite, etc.)
    * querying schema version and database character sets
    * get diskspace available
    * timestamping
    * creating tarball (may take some time): /tmp/satellite-debug.tar.bz2
    * removing temporary debug tree

Debug dump created, stored in /tmp/satellite-debug.tar.bz2
Deliver the generated tarball to your Red Hat Network contact or support
channel.
```

Danach versenden Sie die neue Datei aus dem **`/tmp/`** Verzeichnis an Ihren Red Hat Vertreter zur umgehenden Diagnose.
Zusätzlich bietet Red Hat ein Befehlszeilen-Tool namens **SoS Report** an, weitläufig auch unter dem Befehlsnamen **`sosreport`** bekannt. Dieses Tool sammelt die Konfigurationsparameters Ihres Proxys, die Protokolldateien und Datenbankinformationen, und sendet alles direkt an Red Hat.
Um dieses Tool für Red Hat Satellite Informationen zu nutzen, muss das **`sos`** Paket installiert sein. Geben Sie als Root **`sosreport -o rhn`** auf dem Satellite Server ein, um einen Report zu erzeugen. Zum Beispiel:

```
[root@satserver ~]# sosreport -o rhn

sosreport (version 1.7)

This utility will collect some detailed  information about the
hardware and  setup of your  Red Hat Enterprise Linux  system.
The information is collected and an archive is  packaged under
/tmp, which you can send to a support representative.
Red Hat will use this information for diagnostic purposes ONLY
and it will be considered confidential information.

This process may take a while to complete.
No changes will be made to your system.

Press ENTER to continue, or CTRL-C to quit.
```

Sie werden anschließend nach dem Anfangsbuchstaben Ihres Vornamens und Ihrem Nachnamen gefragt, dann nach einer Support-Ticketnummer (auch Issue-Tracker-Nummer genannt).
Es kann einige Minuten dauern, bis das System den Bericht erzeugt und in einer komprimierten Datei abgespeichert hat. Sobald dieser Vorgang abgeschlossen ist, emailen Sie die neue Datei im **/tmp/** Verzeichnis zur umgehenden Diagnose an Ihren Red Hat Vertreter.

Probes

Monitoring-berechtigte Systeme können Probes an ihnen angewandt haben, welche ständig ihren einwandfreien Zustand und volle Funktionsfähigkeit bestätigen. Dieser Abschnitt listet die verfügbaren Probes, nach Befehls-Gruppe (wie beispielsweise Apache) unterteilt, auf.

Viele Probes, die interne Aspekte Ihres Systems überwachen (wie beispielsweise die Linux::Disk Usage Probe) statt externe Aspekte (wie beispielsweise die Network Services::SSH Probe), erfordern die Installation des Red Hat Network monitoring daemon (**`rhnmd`**). Diese Voraussetzung ist in der individuellen Probe-Referenz vermerkt.

Jede Probe hat ihre eigene Referenz in diesem Abschnitt, in der die erforderlichen Felder (markiert mit *), Standardwerte und die Grenzwerte zum Auslösen von Warnmeldungen identifiziert werden. Zu Beginn eines jeden Abschnitts der unterschiedlichen Befehlsgruppen sind Informationen aufgeführt, die auf alle Probes in dieser Gruppe zutreffen. Abschnitt Abschnitt A.1, „Probe-Richtlinien“ behandelt allgemeine Richtlinien. Die verbleibenden Abschnitte befassen sich mit individuellen Probes.

Anmerkung

Beinahe alle Probes verwenden das *Transmission Control Protocol* (TCP) als Transportprotokoll. Ausnahmen davon werden eigens in den Referenzen der jeweiligen Probes angegeben.

A.1. Probe-Richtlinien

Die folgenden allgemeinen Richtlinien umreißen die Bedeutung eines jeden Probe-Status und stellen eine Anleitung zur Festlegung von Grenzwerten dar.

Die folgende Liste liefert eine kurze Beschreibung der Bedeutung eines jeden Probe-Status:

Unbekannt

Diese Probes können die Messdaten nicht sammeln, die zur Bestimmung des Probe-Status benötigt werden. Die meisten Probes, wenn auch nicht alle, gehen in diesen Status über, wenn ihr Timeout-Wert überschritten wird. Probes mit diesem Status sind unter Umständen nicht korrekt konfiguriert.

Ausstehend

Für diese Probes hat der Red Hat Satellite noch keine Daten erhalten. Es ist normal, dass sich neue Probes in diesem Status befinden. Wenn jedoch alle Probes in diesen Status übergehen, kann es sein, dass die Monitoring-Infrastruktur fehlerhaft ist.

OK

Diese Probes sind erfolgreich ohne Fehler gelaufen. Dies ist der gewünschte Status für alle Probes.

Warnung

Probes, die ihre WARNUNG-Grenzwerte überschritten haben.

Kritisch

Diese Probes haben ihre KRITISCH-Grenzwerte überschritten oder sind aus anderen Gründen

in einen kritischen Status übergegangen. (Manche Probes gehen in den Status KRITISCH über, wenn ihr Timeout-Wert überschritten wurde.)

Seien Sie vorsichtig bei der Auswahl der Grenzwerte. Wenn diese überschritten werden, sollten Sie über ein Problem innerhalb Ihrer Infrastruktur benachrichtigt werden. Timeout-Werte werden grundsätzlich in Sekunden eingegeben. Es gibt auch hier Ausnahmen, die in den einzelnen Probe-Referenzen vermerkt sind.

Wichtig

Die Grenzwerte einiger Probes basieren auf Zeit. Hierbei dürfen die Grenzwerte für KRITISCH und WARNUNG nicht eine größere Zeitspanne erlauben, als diejenige, die für den Timeout-Wert gewählt wurde. Andernfalls wird ein Status UNKNOWN in allen Fällen der erweiterten Latenz zurückgegeben, wodurch die Grenzwerte beseitigt werden. Aus diesem Grund wird von Red Hat dringend empfohlen, dass alle Timeout-Werte über die festgelegte Zeitspanne aller zeitabhängigen Grenzwerte hinausgehen.

Lassen Sie Ihre Probes für eine gewisse Zeit lang ohne Benachrichtigungen laufen, um ein Basis-Leistungsverhalten für jedes Ihrer Systeme herzustellen. Obwohl sich die Standardwerte für Probes für Ihre Zwecke eignen können, so hat jede Organisation eine unterschiedliche Umgebung, die eventuell das Abändern der Grenzwerte erforderlich macht.

A.2. Apache 1.3.x und 2.0.x

Die Probes in diesem Abschnitt können auf Instanzen des Apache Web Servers angewendet werden. Obwohl die Grundeinstellungen davon ausgehen, dass Sie Standard-HTTP verwenden, können Sie auch eine sichere Verbindung wählen, indem Sie das Protokoll **`https`** und Port **`443`** verwenden.

A.2.1. Apache::Processes

Die Apache::Processes Probe überwacht die Prozesse, die auf einem Apache Web Server ausgeführt werden und sammelt folgende Messdaten:

- Pro Child übertragene Daten - Zeichnet Informationen zur Datenübertragung basierend auf individuellen Child-Prozessen auf. Ein sogenannter Child-Prozess entsteht aus dem Parent-Prozess oder einem anderen Prozess heraus.
- Übertragene Daten pro Slot - Die kumulative Datenmenge, die von einem Child-Prozess übertragen wird, der gerade neu startet. Die Anzahl der Slots ist in der **`httpd.conf`** Datei mittels der Einstellung **`MaxRequestsPerChild`** konfiguriert.

Die **`ExtendedStatus`** Direktive in der **`httpd.conf`** Datei des Webservers muss auf **`On`** gesetzt sein, damit diese Probe einwandfrei laufen kann.

Tabelle A.1. Einstellungen für Apache::Processes

Feld	Wert
Application Protocol* (Applikationsprotokoll*)	http
Port*	80
Pathname* (Pfadname*)	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Benutzername	
Passwort	
Timeout*	15
Critical Maximum Megabytes Transferred Per Child (Kritsch - Maximum Megabytes pro Child übertragen)	
Warning Maximum Megabytes Transferred Per Child (Warnung - Maximum Megabytes pro Child übertragen)	
Critical Maximum Megabytes Transferred Per Slot (Kritisch Maximum Megabytes pro Slot übertragen)	
Warning Maximum Megabytes Transferred Per Slot (Warnung Maximum Megabytes pro Slot übertragen)	

A.2.2. Apache::Traffic

Der Apache::Traffic Probe überwacht die Anfragen auf einem Apache Web Server und sammelt folgende Messdaten:

- Aktuelle Anfragen - Die Anzahl an Anfragen, die vom Server während der Laufzeit der Probe durchgeführt werden.
- Anfrage-Rate - Die Zugriffe auf den Server pro Sekunde seitdem die Probe zuletzt durchgeführt wurde.
- Datenverkehr - Die Kilobytes pro Sekunde an Datenverkehr, der vom Server abgewickelt wurde, seitdem die Probe zuletzt durchgeführt wurde.

Die **`ExtendedStatus`** Direktive in der **`httpd.conf`** Datei des Webservers muss auf **`On`** gesetzt sein, damit diese Probe einwandfrei laufen kann.

Tabelle A.2. Apache::Traffic Einstellungen

Feld	Wert
Application Protocol* (Applikationsprotokoll*)	http
Port*	80
Pathname* (Pfadname*)	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Benutzername	
Passwort	
Timeout*	15
Critical Maximum Current Requests (number) (Kritisch - Maximale aktuelle Anfragen (Anzahl))	
Warning Maximum Current Requests (number) (Warnung - Maximale aktuelle Anfragen (Anzahl))	
Critical Maximum Request Rate (events per second) (Kritisch - Maximale Anfrage-Rate (Events pro Sekunde))	
Warning Maximum Request Rate (events per second) (Warnung - Maximale Anfrage-Rate (Events pro Sekunde))	
Critical Maximum Traffic (kilobytes per second) (Kritisch - Maximaler Datenverkehr (Kilobytes pro Sekunde))	
Warning Maximum Traffic (kilobytes per second) (Warnung - Maximaler Datenverkehr (Kilobytes pro Sekunde))	

A.2.3. Apache::Uptime

Der Apache::Uptime Probe speichert die kumulative Betriebszeit, seit der Web-Server zuletzt gestartet wurde. Von dieser Probe werden keine Messdaten gesammelt, da diese dazu entwickelt wurde, Leistungsvereinbarungen oder sogenannte Service Level Agreements (SLAs) nachzuverfolgen.

Tabelle A.3. Apache::Uptime Einstellungen

Feld	Wert
Application Protocol* (Applikationsprotokoll*)	http
Port*	80
Pathname* (Pfadname*)	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Benutzername	
Passwort	
Timeout*	15

A.3. BEA WebLogic 6.x und höher

Die Probes in diesem Abschnitt (mit Ausnahme von JDBC Connection Pool) können dahingehend konfiguriert werden, dass diese die Eigenschaften eines BEA WebLogic 6.x (oder höher) (Administration

oder Management), der auf einem bestimmten Host abläuft, sogar in einer geclusterten Umgebung überwachen. Die Überwachung eines Clusters erfolgt durch das Senden aller SNMP-Abfragen zum Administrations-Server der Domäne und dem darauffolgenden Abfragen der davon verwalteten Server nach individuellen Daten.

Dieser hohe Grad an Detailgenauigkeit kann nur dadurch erreicht werden, indem der **`BEA Domain Admin Server`** Parameter dazu benutzt wird, um zwischen dem Administrations-Server, welcher SNMP-Abfragen erhält, und dem 'Managed'-Server, an dem diese spezielle Probe durchgeführt wird, zu unterscheiden. Wenn eine Probe an einem Administrations-Server durchgeführt werden soll, kann der **`BEA Domain Admin Server`** Parameter ausgelassen werden, damit die Probe sowie auch die SNMP-Abfragen nur an diesen Server gesandt werden.

Wenn es sich beim Host um einen 'Managed'-Server handelt, dann sollte die IP-Adresse des Administrations-Servers im **`BEA Domain Admin Server`** Parameter angegeben werden. Der Name des Managed-Servers sollte im **`BEA Server Name`** Parameter eingefügt werden und and am Ende des **`SNMP Community String`** Feldes angehängt werden. Dadurch werden SNMP-Abfragen zum Administrations-Server Host gesandt. Die Probe wird jedoch zum Managed-Server Host umgeleitet.

Bitte beachten Sie, dass der sogenannte Community String so aussehen sollte **`community_prefix@managed_server_name`**, damit die SNMP-Abfrage Ergebnisse für den gewünschten Managed-Server zurücksenden kann. Schlussendlich muss SNMP auf jedem überwachten System eingeschaltet werden. SNMP-Support kann durch die WebLogic-Konsole eingeschaltet und konfiguriert werden.

Siehe für weitere Informationen über BEA's Community-String Namens-Konventionen die Dokumentation, die mit Ihrem BEA Server kam oder Informationen über die BEA Website.

A.3.1. BEA WebLogic::Execute Queue

Der BEA WebLogic::Execute Queue Probe überwacht die WebLogic Execute Queue und liefert folgende Messdaten:

- Idle Execute Threads - Die Anzahl von Ausführungs-Threads im idle-Status.
- Queue Length - Die Anzahl von Anfragen in der Warteschlange.
- Request Rate - Die Anzahl von Anfragen pro Sekunde.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.4. BEA WebLogic::Execute Queue Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Queue Name*	default
Critical Maximum Idle Execute Threads (Kritisch-Maximum Idle Threads)	
Warning Maximum Idle Execute Threads	
Critical Maximum Queue Length	
Warning Maximum Queue Length	
Critical Maximum Request Rate	
Warning Maximum Request Rate	

A.3.2. BEA WebLogic::Heap Free

Die BEA WebLogic::Heap Free Probe sammelt folgende Messdaten:

- Heap Free - Der Prozentsatz von freiem Heap-Speicher.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.5. BEA WebLogic::Heap Free Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Critical Maximum Heap Free (Kritisch - Maximaler freier Heap)	
Warning Maximum Heap Free (Warnung - Maximaler freier Heap)	
Warning Minimum Heap Free (Warnung - Minimaler freier Heap)	
Critical Minimum Heap Free (Kritisch - Minimaler freier Heap)	

A.3.3. BEA WebLogic::JDBC Connection Pool

Die BEA WebLogic::JDBC Connection Pool Probe überwacht den Java Database Connection (JDBC) Pool nur auf einem Admin-Server (keine Managed Server) und sammelt folgende Messdaten:

- Connections - Die Anzahl der Verbindungen mit JDBC.

- Connections Rate - Die Geschwindigkeit mit der Verbindungen mit JDBC gemacht werden, in Verbindungen pro Sekunde gemessen.
- Waiters - Die Anzahl von Sessions, die darauf warten, mit JDBC verbunden zu werden

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.6. BEA WebLogic::JDBC Connection Pool Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
JDBC Pool Name*	MyJDBC Connection Pool
Critical Maximum Connections (Kritisch - Maximale Verbindungen)	
Warning Maximum Connections (Warnung - Maximale Verbindungen)	
Critical Maximum Connection Rate (Kritisch -Maximale Verbindungsrate)	
Warning Maximum Connection Rate (Warnung - Maximale Verbindungsrate)	
Critical Maximum Waiters (Kritisch - Maximale Waiters9	
Critical Maximum Waiters (Warnung - Maximale Waiters)	

A.3.4. BEA WebLogic::Server State

Der BEA WebLogic::Server State Probe überwacht den aktuellen Status eines BEA Weblogic Webservers. Wenn die Probe keine Verbindung zum Server herstellen kann, hat dies einen KRITISCH-Status zur Folge.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.7. BEA WebLogic::Server State Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	

A.3.5. BEA WebLogic::Servlet

Die BEA WebLogic::Servlet Probe überwacht die Performance eines bestimmten Servlets auf einem WebLogic-Server und sammelt folgende Messdaten:

- High Execution Time - Der längste Zeitraum in Millisekunden, den das Servlet seit dem Starten des

Systems benötigt einen Arbeitsvorgang auszuführen.

- Low Execution Time - Der kürzeste Zeitraum in Millisekunden, den das Servlet seit dem Starten des Systems benötigt einen Arbeitsvorgang auszuführen.
- Execution Time Moving Average - Ein gleitender Durchschnittswert der Durchführungszeit.
- Execution Time Average - Ein Standard-Durchschnitt der Durchführungszeit.
- Reload Rate - Wie oft das spezifizierte Servlet pro Minute neu geladen wird.
- Invocaton Rate - Wie oft das spezifizierte Servlet pro Minute aufgerufen wurde.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.8. BEA WebLogic::Servlet Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Servlet Name*	
Critical Maximum High Execution Time (Kritsch - Maximale Höchstdauer der Ausführung)	
Warning Maximum High Execution Time (Warnung - Maximale Höchstdauer der Ausführung)	
Critical Maximum Execution Time Moving Average (Kritisch - Maximaler gleitender Durchschnittswert der Ausführungsdauer)	
Warning Maximum Execution Time Moving Average (Warnung - Maximaler gleitender Durchschnittswert der Ausführungsdauer)	

A.4. Allgemein

Die Probes in diesem Abschnitt wurden entwickelt um grundsätzliche Aspekte Ihrer Systeme zu überwachen. Wenn Sie diese anwenden, gehen Sie sicher, dass deren zeitlich festgelegte Grenzwerte nicht die Dauer der Timeout-Perioden überschreiten. Ansonsten gibt die Probe einen UNBEKANNT Status in allen Fällen der erweiterten Latenz zurück, wodurch die Grenzwerte beseitigt werden.

A.4.1. General::Remote Program

Der General::Remote Program Probe ermöglicht es Ihnen, jeglichen Befehl oder jegliches Skript auf Ihrem System laufen zu lassen und einen Status-String zu erhalten. Beachten Sie bitte, dass die daraus resultierende Mitteilung auf 1024 Bytes beschränkt ist.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.9. General::Remote Program Einstellungen

Feld	Wert
Command* (Befehl*)	
OK Exit Status*	0
Warning Exit Status* (Warnung Exit Status*)	1
Critical Exit Status* (Kritisch Exit Status*)	2
Timeout	15

A.4.2. General::Remote Program with Data

Die General::Remote Program with Data Probe ermöglicht Ihnen jeglichen Befehl oder jegliches Skript auf Ihrem System laufen zu lassen und einen Wert sowie auch einen Status-String zu erhalten. Dazu müssen Sie XML-Code in Ihr Skript einfügen. Dieser Probe unterstützt folgende XML-Tags:

- <perldata> </perldata>
- <hash> </hash>
- <item key =" "> </item>

Dieses Programm muss einige Wiederholungen des folgenden Codes auf **`STDOUT`** umlenken:

```
<perldata> <hash> <item
key="data">10</item> <item
key="status_message">status message here</item>
</hash> </perldata>
```

Der erforderliche Wert für **`data`** ist der Datenpunkt, der in die Datenbank zu Time-Series Trending Zwecken eingefügt werden muss. Die Option **`status_message`** ist ein optionaler freier Text-String mit maximal 1024 Bytes. Remote Programme, die keine **`status_message`** Option beinhalten, werden immer noch Wert und Status rückmelden.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe ausführen zu können. XML unterscheidet zwischen Groß- und Kleinschreibung. Der **`data`** Element Schlüssel-Name kann nicht verändert werden und muss eine Nummer als seinen Wert erfassen.

Tabelle A.10. General::Remote Program with Data Einstellungen

Feld	Wert
Command* (Befehl*)	
OK Exit Status*	0
Warning Exit Status* (Warnung Exit Status*)	1
Critical Exit Status* (Kritisch Exit Status*)	2
Timeout	15

A.4.3. General::SNMP Check

Der General::SNMP Check Probe testet Ihren SNMP-Server durch Angabe einer einzelnen Objekt-ID (OID) in punktierter Schreibweise (z.B. **`1.3.6.1.2.1.1.1.0`**) sowie einen Grenzwert zum Rückgabewert. Er sammelt die folgenden Messdaten:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der SNMP-Server auf eine Verbindungsanfrage antwortet.

Anforderungen - SNMP muss auf den zu überwachenden Systemen laufen, damit diese Probe ausgeführt werden kann. Es können nur Ganzzahlen als Grenzwerte verwendet werden.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.11. General::SNMP Check Einstellungen

Feld	Wert
SNMP OID*	
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	2
Timeout*	15
Critical Maximum Value (Kritisch - Maximaler Wert)	
Warning Maximum Value (Warnung - Maximaler Wert)	
Warning Minimum Value (Warnung - Minimaler Wert)	
Critical Minimum Value (Kritisch - Minimaler Wert)	

A.4.4. General::TCP Check

Die General::TCP Check Probe testet Ihren TCP-Server, indem sichergestellt wird, dass dieser sich via der angegebenen Portnummer mit einem System verbinden kann. Die folgenden Messdaten werden gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der TCP-Server auf eine Verbindungsanfrage antwortet.

Nach Herstellung einer Verbindung gibt die Probe den String weiter, welcher im **`Send (Sende)`** Feld angegeben wurde. Die Probe erwartet eine Rückantwort vom System, welche den Substring enthalten sollte, der im **`Expect (Erwarte)`** Feld festgelegt ist. Wenn der erwartete String nicht gefunden wird, dann meldet die Probe einen KRITISCHEN-Status zurück.

Tabelle A.12. General::TCP Check Einstellungen

Feld	Wert
Send (Sende)	
Expect (Erwarte)	
Port*	1
Timeout*	10
Critical Maximum Latency (Kritisch Maximale Latenz)	
Warning Maximum Latency (Warnung Maximale Latenz)	

A.4.5. General::UDP Check (General::UDP Check)

Der General::UDP Check Probe testet Ihren UDP-Server, indem sichergestellt wird, dass dieser sich via der festgesetzten Portnummer mit einem System verbinden kann. Die folgenden Messdaten werden

gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der UDP-Server auf eine Verbindungsanfrage antwortet.

Nach Herstellung einer Verbindung gibt die Probe den String weiter, welcher im **Send (Sende)** Feld angegeben wurde. Die Probe erwartet eine Rückantwort vom System, welche den Substring enthalten sollte, der im **Expect (Erwarte)** Feld festgelegt ist. Wenn der erwartete String nicht gefunden wird, dann meldet die Probe einen KRITISCHEN-Status zurück.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.13. General::UDP Check Einstellungen

Feld	Wert
Port*	1
Send (Sende)	
Expect (Erwarte)	
Timeout*	10
Critical Maximum Latency (Kritisch Maximale Latenz)	
Warning Maximum Latency (Warnung Maximale Latenz)	

A.4.6. General::Uptime (SNMP)

Der General::Uptime (SNMP) Probe zeichnet die Zeitspanne auf, seitdem die Einheit zuletzt gestartet wurde. Dabei wird der SNMP Object Identifier (OID) verwendet, um zu diesem Wert zu gelangen. Der einzige Fehlerstatus ist in diesem Fall UNBEKANNT.

Anforderungen - SNMP muss auf dem zu überwachenden System laufen und der Zugang zum OID muss freigegeben sein, um diese Probe ausführen zu können.

Das Transportprotokoll dieser Probe ist UDP (User Datagram Protokoll).

Tabelle A.14. General::Uptime (SNMP) Einstellungen

Feld	Wert
SNMP Community String*	öffentlich
SNMP Port*	161
SNMP Version*	2
Timeout*	15

A.5. Linux

Die Probes in diesem Abschnitt überwachen essentielle Aspekte Ihres Linux-Systems vom CPU-Verbrauch bis zum virtuellen Speicher. Wenden Sie diese an unternehmenswichtigen Systemen an, um frühzeitig Warnungen zu erhalten.

Im Gegensatz zu anderen Probe-Gruppen, die den Red Hat Network monitoring daemon benötigen oder nicht, ist die Vorraussetzung für jede Linux-Probe, dass der **rhnmd** Daemon auf dem zu überwachenden System läuft.

A.5.1. Linux::CPU Usage

Der Linux::CPU Usage Probe überwacht die CPU-Auslastung auf einem System und sammelt folgende Messdaten:

- CPU Percent Used - Der fünf Sekunden lang gemessene Durchschnitt des CPU Prozentsatzes, der bei der Ausführung der Probe gemessen wird.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diese Probe auszuführen.

Tabelle A.15. Linux::CPU Usage Einstellungen

Feld	Wert
Timeout*	15
Critical Maximum CPU Percent Used (Kritisch - Maximaler verwendeter CPU Prozentsatz)	
Warning Maximum CPU Percent Used (Warnung - Maximaler Verwendeter CPU Prozentsatz)	

A.5.2. Linux::Disk IO Throughput

Der Linux::Disk IO Throughput Probe überwacht eine Disk und sammelt folgende Messdaten:

- Read Rate - Die Menge an Daten die, in Kilobytes gemessen, pro Sekunde gelesen werden.
- Write Rate - Die Menge an Daten die, in Kilobytes gemessen, pro Sekunde geschrieben werden.

Um die Werte für das Mussfeld **Disk number or disk name (Plattennummer oder Plattenname)** zu erhalten, führen Sie **iostat** auf dem zu überwachenden System aus. Der Standardwert **0** liefert für gewöhnlich Statistiken über die erste Festplatte, die direkt mit dem System verbunden ist.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen. Ebenso muss der **Disk number or disk name (Plattennummer oder Plattenname)** Parameter mit dem Format übereinstimmen, welches beim Ausführen von **iostat** angezeigt wird. Wenn das Format nicht identisch ist, dann geht die konfigurierte Probe in einen UNBEKANNT-Status.

Tabelle A.16. Linux::Disk IO Throughput Einstellungen

Feld	Wert
Disk number or disk name* (Plattennummer oder Plattenname)	0
Timeout*	15
Critical Maximum KB read/second (Kritisch - Maximale KB gelesen/Sekunde)	
Warning Maximum KB read/second (Warnung - Maximale KB gelesen/Sekunde)	
Warning Minimum KB read/second (Warnung - Minimale KB gelesen/Sekunde)	
Critical Minimum KB read/second (Kritisch Minimale KB gelesen/Sekunde)	
Critical Maximum KB written/second (Kritisch - Maximale KB geschrieben/Sekunde)	
Warning Maximum KB written/second (Warnung - Maximale KB geschrieben/Sekunde)	
Warning Minimum KB written/second (Warnung - Minimale KB geschrieben/Sekunde)	
Critical Minimum KB written/second (Kritisch - Minimale KB geschrieben/Sekunde)	

A.5.3. Linux::Disk Usage

Die Linux::Disk Usage Probe überwacht den Plattenplatz auf einem spezifischen Dateisystem und sammelt folgende Messdaten:

- File System Used - Der Prozentsatz des aktuell verwendeten Dateisystems.
- Space Used - Die Menge des Dateisystems in Megabyte, welche aktuell verwendet wird.
- Space Available - Die Menge des Dateisystems in Megabyte, welche aktuell zur Verfügung steht.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.17. Linux::Disk Usage Einstellungen

Feld	Wert
File System* (Dateisystem*)	/dev/hda1
Timeout*	15
Critical Maximum File System Percent Used (Kritisch - Maximal verwendeter Prozentsatz des Dateisystems)	
Warning Maximum File System Percent Used (Warnung - Maximal verwendeter Prozentsatz des Dateisystems)	
Critical Maximum Space Used (Kritisch - Maximal verwendeter Platz)	
Warning Maximum Space Used (Warnung - Maximal verwendeter Platz)	
Warning Minimum Space Available (Warnung - Minimal verfügbarer Platz)	
Critical Minimum Space Available (Kritisch - Minimal verfügbarer Platz)	

A.5.4. Linux::Inodes

Der Linux::Inodes Probe überwacht das jeweilige Dateisystem und sammelt folgende Messdaten:

- Inodes - Der Prozentsatz an Inodes, die sich aktuell in Verwendung befinden

Inode ist eine Datenstruktur, die Informationen über Dateien in einem Linux-Dateisystem enthält. Es gibt eine Inode für jede Datei und eine Datei ist einzigartig durch das Dateisystem gekennzeichnet, auf dem diese sich befindet, sowie durch die Inode-Nummer auf diesem System.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.18. Linux::Inodes Einstellungen

Feld	Wert
File System* (Dateisystem*)	/
Timeout*	15
Critical Maximum Inodes Percent Used (Kritisch - Maximal verwendeter Prozentsatz an Inodes)	
Warning Maximum Inodes Percent Used (Warnung - Maximal verwendeter Prozentsatz an Inodes)	

A.5.5. Linux::Interface Traffic

Der Linux::Interface Traffic Probe misst den Verkehr an der festgelegten Schnittstelle (beispielsweise eth0) und sammelt die folgenden Messdaten:

- Input Rate - Der in Bytes pro Sekunde gemessene Verkehr, der an der entsprechenden Schnittstelle eingeht.
- Output Rate - Der in Bytes pro Sekunde gemessene Verkehr, der von der entsprechenden Schnittstelle ausgeht.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.19. Linux::Interface Traffic Einstellungen

Feld	Wert
Interface * (Schnittstelle*)	
Timeout*	30
Critical Maximum Input Rate (Kritisch - Maximale Eingangsrate)	
Warning Maximum Input Rate (Warnung - Maximale Eingangsrate)	
Warning Minimum Input Rate (Warnung - Minimale Eingangsrate)	
Critical Minimum Input Rate (Kritisch - Minimale Eingangsrate)	
Critical Maximum Output Rate (Kritisch - Maximale Ausgangsrate)	
Warning Maximum Output Rate (Warnung - Maximale Ausgangsrate)	
Warning Minimum Output Rate (Warnung - Minimale Ausgangsrate)	
Critical Minimum Output Rate (Kritisch - Minimale Ausgangsrate)	

A.5.6. Linux::Load

Der Linux::Load Probe überwacht die CPU eines Systems und sammelt die folgenden Messdaten:

- Last - Die durchschnittlich Last auf der System-CPU über unterschiedliche Zeiträume hinweg.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.20. Linux::Load Einstellungen

Feld	Wert
Timeout*	15
Critical CPU Load 1-minute average (Kritisch - CPU-Last 1-minütiger Durchschnitt)	
Warning CPU Load 1-minute average (Warnung - CPU-Last 1-minütiger Durchschnitt)	
Critical CPU Load 5-minute average (Kritisch - CPU-Last 5-minütiger Durchschnitt)	
Warning CPU Load 5-minute average (Warnung - CPU-Last 5-minütiger Durchschnitt)	
Critical CPU Load 15-minute average (Kritisch - CPU-Last 15-minütiger Durchschnitt)	
Warning CPU Load 15-minute average (Warnung - CPU-Last 15-minütiger Durchschnitt)	

A.5.7. Linux::Memory Usage

Der Linux::Memory Usage Probe überwacht den Speicher auf einem System und sammelt die folgenden Messdaten:

- RAM Free - Die Menge an freiem RAM auf einem System in Megabytes.

Sie können auch den nutzbaren Speicher miteinbeziehen, indem Sie einfach **`yes`** oder **`no`** in das **`Include reclaimable memory`** Feld eingeben.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.21. Linux::Memory Usage Einstellungen

Feld	Wert
Include reclaimable memory (nutzbaren Speicher miteinbeziehen)	nein
Timeout*	15
Warning Maximum RAM Free (Warnung - Maximaler freier RAM)	
Critical Maximum RAM Free (Kritisch - Maximaler freier RAM)	

A.5.8. Linux::Process Counts by State

Der Linux::Process Counts by State Probe legt die Anzahl von Prozessen in den folgenden Status fest:

- Blocked (Blockiert) - Ein Prozess, der in die Warteschlange verschoben wurde und dessen Status auf **`waiting`** geändert wurde.
- Defunct (Nicht mehr bestehend) - Ein abgebrochener Prozess (entweder von einem Signal abgebrochen oder weil er **`exit()`** aufgerufen hat), dessen Elternprozess noch keine Benachrichtigung über den Abbruch erhalten hat, indem eine Form des **`wait()`** Systemaufrufs

ausgeführt wurde.

- Stopped (Angehalten) - Ein Prozess der noch vor der vollständigen Ausführung angehalten wurde.
- Sleeping (Ruhezustand) - Ein Prozess, der sich im **`Interruptible`** (unterbrechbaren) Ruhezustand befindet, der später wieder in den Speicher eingeführt werden kann und die Ausführung dort wieder aufnimmt, wo er aufgehört hat.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.22. Linux::Process Counts by State Einstellungen

Feld	Wert
Timeout*	15
Critical Maximum Blocked Processes (Kritisch - Maximal gesperrte Prozesse)	
Warning Maximum Blocked Processes (Warnung - Maximal gesperrte Prozesse)	
Critical Maximum Defunct Processes (Kritisch - Maximal nicht mehr bestehende Prozesse)	
Warning Maximum Defunct Processes (Warnung - Maximal nicht mehr bestehende Prozesse)	
Critical Maximum Stopped Processes (Kritisch - Maximal angehaltene Prozesse)	
Warning Maximum Stopped Processes (Warnung - Maximale Angehaltene Prozesse)	
Critical Maximum Sleeping Processes (Kritisch - Maximal schlafende Prozesse)	
Warning Maximum Sleeping Processes (Warnung - Maximal schlafende Prozesse)	
Critical Maximum Child Processes (Kritisch - Maximale Kindprozesse)	
Warning Maximum Child Processes (Warnung - Maximale Kindprozesse)	

A.5.9. Linux::Process Count Total

Der Linux::Process Count Total Probe überwacht ein System und sammelt folgende Messdaten:

- Process Count - Die Gesamtanzahl der Prozesse, die gegenwärtig auf dem System laufen.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.23. Linux::Process Count Total Einstellungen

Feld	Wert
Timeout*	15
Critical Maximum Process Count (Kritisch - Maximale Anzahl der Prozesse)	
Warning Maximum Process Count (Warnung - Maximale Anzahl der Prozesse)	

A.5.10. Linux::Process Health

Der Linux::Process Health Probe überwacht benutzerspezifische Prozesse und sammelt die folgenden Messdaten:

- CPU Usage - Die CPU-Verbrauchsrate für einen bestimmten Prozess in Millisekunden pro Sekunde. Diese Messdaten berichten über die Zeit Spalte der **ps** Ausgabe, welche die kumulative CPU-Zeit ist, die vom Prozess benötigt wird. Dies macht die Messdaten unabhängig vom Probe-Intervall, ermöglicht einen sinnvollen Grenzwert zu setzen und erstellt brauchbare Diagramme (beispielsweise wird eine plötzliche Spitze im CPU-Verbrauch als Spitze im Diagramm angezeigt).
- Child Process Groups - Die Anzahl von Kindprozessen, die vom spezifizierten Elternprozess erzeugt werden. Ein Kindprozess übernimmt die meisten Attribute, wie beispielsweise offene Dateien, vom seinem Elternprozess.
- Threads - Die Anzahl laufender Threads für einen bestimmten Prozess. Ein Thread ist ein Ausführungsstrang innerhalb eines Prozesses (Grundeinheit der CPU-Auslastung) und besteht aus einem sogenannten Befehlszähler, einem Register-Satz und einem Stacksegment. Ein Thread wird auch als 'Leichtgewichtprozess' bezeichnet.
- Physical Memory Used - Die Menge an physischem Speicher (oder RAM) in Kilobytes, die vom angegebenen Prozess verwendet wird.
- Virtual Memory Used (Verbrauchter virtueller Speicher) - Die Menge an virtuellem Speicher in Kilobytes, die vom angegebenen Prozess verwendet wird oder die Größe des Prozesses in Realspeicher plus Swap.

Legen Sie den Prozess entweder anhand dem Befehlsnamen oder der Prozess ID (PID) fest. Wenn Sie eine PID eingeben, dann übersteuert diese den Befehlsnamen. Wenn weder Befehlsname noch PID eingetragen sind, wird der Fehler Command not found (Befehl nicht gefunden) angezeigt und die Probe auf den KRITISCH Status gesetzt.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.24. Linux::Process Health Einstellungen

Feld	Wert
Command Name (Befehlsname)	
Process ID (PID) file (Prozess ID (PID) Datei)	
Timeout*	15
Critical Maximum CPU Usage (Kritisch - Maximaler CPU-Verbrauch)	
Warning Maximum CPU Usage (Warnung - Maximaler CPU-Verbrauch)	
Critical Maximum Child Process Groups (Kritisch - Maximale Kindprozess-Gruppen)	
Warning Maximum Child Process Groups (Warnung - Maximale Kindprozess-Gruppen)	
Critical Maximum Threads (Kritisch - Maximale Threads)	
Warning Maximum Threads (Warnung - Maximale Threads)	
Critical Maximum Physical Memory Used (Kritisch - Maximal verbrauchter physischer Speicher)	
Warning Maximum Physical Memory Used (Warnung - Maximal verbrauchter physischer Speicher)	
Critical Maximum Virtual Memory Used (Kritisch - Maximaler verbrauchter virtueller Speicher)	
Warning Maximum Virtual Memory Used (Warnung - Maximaler verbrauchter virtueller Speicher)	

A.5.11. Linux::Process Running

Der Linux::Process Running Probe überprüft, ob der angegebene Prozess einwandfrei abläuft. Dabei werden entweder Prozesse oder Prozessgruppen gezählt. Dies hängt davon ab, ob das Kontrollfeld **`Anzahl Prozessgruppen`** ausgewählt ist.

Standardmäßig ist das Kontrollfeld ausgewählt, wodurch angezeigt wird, dass die Probe die Anzahl von Prozessgruppenführern unabhängig von der Anzahl von Kindern zählen soll. Dies ermöglicht es Ihnen beispielsweise zu überprüfen, ob zwei separate Apache Web Server ungeachtet der (dynamischen) Anzahl an Kindprozessen laufen. Wenn diese Auswahl nicht getroffen wurde, dann führt die Probe eine direkte Zählung der Anzahl von Prozessen (Kinder und Eltern), die dem angegebenen Prozess entsprechen, durch.

Legen Sie den Prozess entweder nach Befehlsname oder Prozess-ID (PID) fest. Wenn Sie eine PID eingeben, dann übersteuert diese den eingegebenen Befehlsnamen. Wenn weder Befehlsname noch PID eingetragen sind, wird die Fehlermeldung Command not found (Befehl nicht gefunden) angezeigt und die Probe auf den KRITISCH Status gesetzt.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.25. Linux::Process Running Einstellungen

Feld	Wert
Befehlsname	
PID-Datei	
Prozessgruppen zählen	(überprüft)
Timeout*	15
Kritisch Maximale Anzahl laufender Prozesse	
Kritisch Minimale Anzahl laufender Prozesse	

A.5.12. Linux::Swap Usage

Der Linux::Swap Usage Probe überwacht die Swap-Partitionen auf einem System und sammelt folgende Messdaten:

- Freier Swap - Der Prozentsatz an derzeit freiem Swap-Speicher.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.26. Linux::Swap Usage Einstellungen

Feld	Wert
Timeout*	15
Warnung Minimaler freier Swap	
Kritisch Minimaler freier Swap	

A.5.13. Linux::TCP Connections by State

Die Linux::TCP Connections by State Probe ermittelt die gesamte Anzahl an TCP-Verbindungen sowie die jeweilige Menge in den folgenden Status:

- TIME_WAIT - Der Socket wartet nach dem Schließen für Übertragungs-Fernabschaltung, damit es noch Pakete verarbeiten kann, die sich noch immer im Netzwerk befinden.
- CLOSE_WAIT - Die externe Anlage wurde abgeschaltet und wartet nunmehr bis der Socket geschlossen ist.
- FIN_WAIT - Der Socket ist geschlossen und die Verbindung wird jetzt abgeschaltet.
- ESTABLISHED - Der Socket hat eine Verbindung aufgebaut.
- SYN_RCVD - Die Verbindungs-Anforderung wurde vom Netzwerk erhalten.

Diese Probe kann dabei hilfreich sein, Netzwerkverkehr aufzufinden und auf spezielle IP-Adressen zu beschränken oder auf das überwachte System eingehende Netzwerkverbindungen genauer zu überprüfen.

Die Filter-Parameter für die Probe erlauben Ihnen den Anwendungsbereich der Probe einzugrenzen. Diese Probe verwendet den **`netstat -ant`** Befehl um Daten abzufragen. Die Parameter **`Lokale IP-Adresse`** und **`Lokaler Port`** verwenden Werte in der **`Local Address`** Spalte der Ausgabe; die **`Remote IP-Adresse`** and **`Remoter Port`** Parameter verwenden Werte in der **`Foreign Address`** Spalte der Ausgabe zur Berichterstattung.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.27. Linux::TCP Connections by State Einstellungen

Feld	Wert
Gefilterte Liste lokaler IP-Adressen	
Filter lokaler Portnummern	
Gefilterte Liste remoter IP-Adressen	
Filter remoter Portnummern	
Timeout*	15
Kritisch Maximale Gesamtverbindungen	
Warnung Maximale Gesamtverbindungen	
Kritisch Maximale TIME_WAIT-Verbindungen	
Warnung Maximale TIME_WAIT-Verbindungen	
Kritisch Maximale CLOSE_WAIT-Verbindungen	
Warnung Maximale CLOSE_WAIT-Verbindungen	
Kritisch Maximale FIN_WAIT-Verbindungen	
Warnung Maximale FIN_WAIT-Verbindungen	
Kritisch Maximale ESTABLISHED-Verbindungen	
Warnung Maximale ESTABLISHED-Verbindungen	
Kritisch Maximale SYN_RCVD-Verbindungen	
Warnung Maximale SYN_RCVD-Verbindungen	

A.5.14. Linux::Users

Der Linux::Users Probe überwacht die Benutzer eines Systems und liefert folgende Messdaten:

- Benutzer - Die Anzahl der derzeit angemeldeten Benutzer.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.28. Linux::Users Einstellungen

Feld	Wert
Timeout*	15
Kritisch Maximale Benutzeranzahl	
Warnung Maximale Benutzeranzahl	

A.5.15. Linux::Virtual Memory

Die Linux::Virtual Memory Probe überwacht den gesamten Systemspeicher und sammelt folgende Messdaten:

- Virtueller Speicher - Der Prozentsatzt des gesamten freien Systemspeichers - RAM plus Swap.

Anforderungen - Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.29. Linux::Virtual Memory Einstellungen

Feld	Wert
Timeout*	15
Warnung Minimaler freier virtueller Speicher	
Kritisch Minimaler freier virtueller Speicher	

A.6. LogAgent

Die Proben in diesem Abschnitt überwachen die Protokolldateien auf Ihren Systemen. Sie können diese dazu verwenden, Protokolle nach bestimmten Ausdrücken (Expressions) abzufragen und die Größe von Dateien zu beobachten. Der **nocpulse** Benutzer muss eine Leseberechtigung für Ihre Protokolldateien besitzen, damit LogAgent Probes ausgeführt werden können.

Beachten Sie, dass Daten vom ersten Durchgang dieser Probes nicht mit den Grenzwerten verglichen werden, um fälschliche Benachrichtigungen zu vermeiden, die von unvollständigen Messdaten hervorgerufen werden. Die Messungen werden beim zweiten Lauf beginnen.

A.6.1. LogAgent::Log Pattern Match

Die LogAgent::Log Pattern Match Probe verwendet reguläre Ausdrücke (Regular Expressions), um Text innerhalb der überwachten Protokolldatei zu vergleichen und sammelt folgende Messdaten:

- Übereinstimmungen bei Anwendung regulärer Ausdrücke - Die Anzahl von Übereinstimmungen, die aufgetreten sind, seitdem die Probe zuletzt gelaufen ist.
- Übereinstimmungsrate bei Anwendung regulärer Ausdrücke - Die Anzahl von Übereinstimmungen pro Minute seitdem die Probe zuletzt gelaufen ist.

Anforderungen — Der Red Hat Network monitoring daemon (**rhnmd**) muss auf dem zu überwachenden System laufen, damit diese Probe ausgeführt werden kann. Damit die Probe laufen kann muss dem **nocpulse** Benutzer Leseberechtigung für Ihre Protokolldateien gegeben werden.

Zusätzlich zum Namen und dem Ort der zu überwachenden Protokolldatei müssen Sie einen regulären Ausdruck im enstprechenden 'Regex'-Format für **egrep** bereitstellen; oder auch **grep -E** für erweiterte reguläre Ausdrücke. Dies ist der reguläre Ausdruck für **egrep**:

```
^ beginning of line
$ end of line
. match one char
* match zero or more chars
[] match one character set, e.g. '[Ff]oo'
[^] match not in set '[^A-F]oo'
+ match one or more of preceding chars
? match zero or one of preceding chars
| or, e.g. a|b
() groups chars, e.g., (foo|bar) or (foo)+
```

Warnung

Fügen Sie keine einzelnen Anführungszeichen (') in den regulären Ausdruck ein. Ansonsten kommt es zum Fehlschlagen von **`egrep`** ohne Benachrichtigung und dementsprechend einer Zeitüberschreitung der Probe.

Tabelle A.30. LogAgent::Log Pattern Match Einstellungen

Feld	Wert
Protokolldatei*	/var/log/messages
Regulärer Ausdruck*	
Timeout*	45
Kritisch Maximale Übereinstimmungen	
Warnung Maximale Übereinstimmungen	
Warnung Minimale Übereinstimmungen	
Kritisch Minimale Übereinstimmungen	
Kritisch Maximale Übereinstimmungsrate	
Warnung Maximale Übereinstimmungsrate	
Warnung Minimale Übereinstimmungsrate	
Kritisch Maximale Übereinstimmungsrate	

A.6.2. LogAgent::Log Size

Die LogAgent::Log Size Probe überwacht Protokolldatei-Wachstum und sammelt folgende Messdaten:

- Größe - Um wieviele Bytes die Größe der Protokolldatei seit der letzten Probe zugenommen hat.
- Ausgaberate - Das Wachstum der Protokolldatei wird in der Anzahl von Bytes pro Minute seit der letzten Messung dargestellt.
- Zeilen - Die Anzahl an Zeilen, die seit der letzten Messung in die Logdatei geschrieben wurden.
- Zeilenrate - Die Anzahl der Zeilen pro Minute, die seit der letzten Messung in die Protokolldatei geschrieben wurden.

Anforderungen — Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem zu überwachenden System laufen, damit diese Probe ausgeführt werden kann. Damit die Probe laufen kann muss dem **`nocpulse`** Benutzer Leseberechtigung für Ihre Protokolldateien gegeben werden.

Tabelle A.31. LogAgent::Log Size Einstellungen

Feld	Wert
Protokolldatei*	/var/log/messages
Timeout*	20
Kritisch Maximale Größe	
Warnung Maximale Größe	
Warnung Minimale Größe	
Kritisch Minimale Größe	
Critical Maximum Output Rate (Kritisch - Maximale Ausgangsrate)	
Warning Maximum Output Rate (Warnung - Maximale Ausgangsrate)	
Warning Minimum Output Rate (Warnung - Minimale Ausgangsrate)	
Critical Minimum Output Rate (Kritisch - Minimale Ausgangsrate)	
Kritisch Maximale Zeilen	
Warnung Maximale Zeilen	
Warnung Maximale Zeilen	
Kritisch Maximale Zeilen	
Kritisch Maximale Zeilenrate	
Warnung Maximale Zeilenrate	
Warnung Minmale Zeilenrate	
Kritisch Minimale Zeilenrate	

A.7. MySQL 3.23 - 3.33

Die Probes in diesem Abschnitt überwachen Aspekte der MySQL-Datenbank unter Verwendung der **`mysqladmin`**-Binärdatei. Für diese Probes sind keine speziellen Benutzerprivilegien erforderlich.

Beachten Sie, dass das **`mysql-server`** Paket auf dem System, dass die Überwachung dieser Probes durchführt, installiert sein muss. Siehe MySQL Installationsabschnitt des *Red Hat Satellite Installationshandbuch* für Instruktionen.

A.7.1. MySQL::Database Accessibility

Die MySQL::Database Accessibility Probe testet die Verbindungsfähigkeit durch einen Datenbank-Account, welcher keine Datenbankprivilegien besitzt. Wenn keine Verbindung hergestellt wird, hat dies einen KRITISCH-Status zur Folge.

Tabelle A.32. MySQL::Database Accessibility Einstellungen

Feld	Wert
Benutzername*	
Passwort	
MySQL Port	3306
Datenbank*	mysql
Timeout	15

A.7.2. MySQL::Opened Tables

Die MySQL::Opened Tables Probe überwacht den MySQL Server und sammelt folgende Messdaten:

- Geöffnete Tabellen - Die Tabellen, die seit dem Starten des Servers geöffnet wurden.

Tabelle A.33. MySQL::Opened Tables Einstellungen

Feld	Wert
Benutzername	
Passwort	
MySQL Port*	3306
Timeout	15
Kritisch Maximale geöffnete Objekte	
Warnung Maximale geöffnete Objekte	
Warnung Minimale geöffnete Objekte	
Kritisch Minimale geöffnete Objekte	

A.7.3. MySQL::Open Tables

Die MySQL::Open Tables Probe überwacht die MySQL Server und sammelt folgende Messdaten:

- Offene Tabellen - Die Anzahl von offenen Tabellen, wenn die Probe läuft.

Tabelle A.34. MySQL::Open Tables Einstellungen

Feld	Wert
Benutzername	
Passwort	
MySQL Port*	3306
Timeout	15
Kritisch Maximale offene Objekte	
Warnung Maximale offene Objekte	
Warnung Minimale offene Objekte	
Kritisch Minimale offene Objekte	

A.7.4. MySQL::Query Rate

Die MySQL::Query Rate Probe überwacht den MySQL Server und sammelt folgende Messdaten:

- Abfragerate - Die durchschnittliche Anzahl von Abfragen pro Sekunde pro Datenbankserver.

Tabelle A.35. MySQL::Query Rate Einstellungen

Feld	Wert
Benutzername	
Passwort	
MySQL Port*	3306
Timeout	15
Kritisch Maximale Abfragerate	
Warnung Maximale Abfragerate	
Warnung Minimale Abfragerate	
Kritisch Minimale Abfragerate	

A.7.5. MySQL::Threads Running

Die MySQL::Threads Running Probe überwacht den MySQL Server und sammelt folgende Messdaten:

- Laufende Threads - Die Gesamtanzahl laufender Threads innerhalb der Datenbank.

Tabelle A.36. MySQL::Threads Running Einstellungen

Feld	Wert
Benutzername	
Passwort	
MySQL Port*	3306
Timeout	15
Kritisch Maximale laufende Threads	
Warnung Maximale laufende Threads	
Warnung Minimale laufende Threads	
Kritisch Minimale laufende Threads	

A.8. Netzwerkdienste

Die Probes in diesem Abschnitt überwachen verschiedenste Dienste, die wesentlich für ein funktionierendes Netzwerk sind. Gehen Sie sicher, dass die zeitlich festgelegten Grenzwerte nicht den Zeitraum überschreiten, der für die Timeout-Periode festgelegt wurde. Ansonsten gibt die Probe einen UNBEKANNT Status in allen Fällen der erweiterten Latenz zurück, wodurch die Grenzwerte beseitigt werden.

A.8.1. Network Services::DNS Lookup

Die Network Services::DNS Lookup Probe benutzt den Befehl **`dig`**, um zu sehen, ob der System- oder Domänenname aufgelöst werden kann, der im Feld **`Host oder Adresse zum Nachsehen`** festgelegt ist. Diese sammelt folgende Messdaten:

- Abfragezeit - Wie lange es dauert, in Millisekunden gemessen, um die **`dig`** Anfrage auszuführen.

Dies ist sehr nützlich bei der Überwachung des Status Ihres DNS-Servers. Wenn Sie einen Ihrer DNS-Server überwachen möchten, geben Sie einen bekannten Host-/Domänennamen ein, wie beispielsweise eine bekannte Suchmaschine oder Firmen-Website.

Tabelle A.37. Network Services::DNS Lookup Einstellungen

Feld	Wert
Host oder Adresse zum Nachsehen	
Timeout*	10
Kritisch Maximale Abfragezeit	
Warnung Maximale Abfragezeit	

A.8.2. Network Services::FTP

Die Network Services::FTP Probe benutzt Netzwerk-Sockets, um FTP Port-Verfügbarkeit zu testen. Die folgenden Messdaten werden gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der FTP-Server auf eine Verbindungs-Anforderung antwortet.

Diese Probe unterstützt Authentifikation. Geben Sie Benutzername und Passwort in die entsprechenden Felder ein. Der optionale **Expect** Wert ist die Zeichenkette mit der nach einer erfolgreich hergestellten Verbindung zum FTP-Server verglichen wird. Wenn diese erwartete Zeichenfolge nicht gefunden werden kann, meldet die Probe einen KRITISCH Status zurück.

Tabelle A.38. Network Services::FTP Einstellungen

Feld	Wert
Expect (Erwarte)	FTP
Benutzername	
Passwort	
FTP Port*	21
Timeout*	10
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.3. Network Services::IMAP Mail

Die Network Services::IMAP Mail Probe ermittelt, ob es mit dem IMAP 4 Dienst auf dem System verbinden kann. Wenn Sie einen optionalen Port eingeben, übersteuert dies den Standard-Port 143. Die folgenden Messdaten werden gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der IMAP-Server auf eine Verbindungs-Anforderung antwortet.

Der erforderliche **Expect** Wert ist die Zeichenfolge, die nach einer erfolgreichen Verbindung zu einem IMAP-Server verglichen wird. Wenn der erwartete String nicht gefunden werden kann, dann meldet die Probe den Status KRITISCH zurück.

Tabelle A.39. Network Services::IMAP Mail Einstellungen

Feld	Wert
IMAP Port*	143
Expect*	OK
Timeout*	5
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.4. Network Services::Mail Transfer (SMTP)

Die Network Services::Mail Transfer (SMTP) Probe ermittelt, ob eine Verbindung zum SMTP-Port auf dem System möglich ist. Die Angabe einer optionalen Portnummer übersteuert den Standard-Port 25. Folgenden Messdaten werden gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der SMTP-Server auf eine Verbindungs-Anforderung antwortet.

Tabelle A.40. Network Services::Mail Transfer (SMTP) Einstellungen

Feld	Wert
SMTP Port*	25
Timeout*	10
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.5. Network Services::Ping

Die Network Services::Ping Probe ermittelt, ob der Red Hat Satellite Server das zu überwachende System oder eine spezielle IP-Adresse mit **`ping`** erreichen kann. Der Paketverlust sowie auch die Zeit, die der Pingvorgang selbst hin- und zurück benötigt, verglichen mit den Warnung- und Kritisch-Grenzwerten, wird ebenso gemessen. Der erforderliche **`Pakete zu versenden`** Wert ermöglicht es Ihnen zu kontrollieren, wieviele ICMP ECHO Pakete zum System gesendet werden. Diese Probe sammelt folgende Messdaten:

- Durchschnittliche Ping-Zeit - Die Zeitspanne in Millisekunden, die vom ICMP ECHO Paket zum überwachten System und zurück benötigt wird.
- Paketverlust - Der Prozentsatz von Daten, die während dem Sendevorgang verloren gehen.

Wenn auch optional, kann das Feld **`IP-Adresse`** beim Sammeln von Messdaten für Systeme mit mehreren IP-Adressen behilflich sein. Wenn das System beispielsweise mit mehreren virtuellen IP-Adressen konfiguriert wird oder Network Address Translation (NAT) verwendet, um interne und externe IP-Adressen zu unterstützen, kann diese Option dazu benutzt werden, eine sekundäre IP-Adresse anstatt der primären IP-Adresse, die mit dem Hostnamen verbunden ist, zu überprüfen.

Beachten Sie, dass diese Probe den **`ping`** Befehl von einem Red Hat Satellite Server und nicht vom überwachten System aus durchführt. Die Eingabe in das IP-Adresses-Feld testet also nicht die Verbindungsfähigkeit zwischen dem System und der festgelegten IP-Adresse, sondern zwischen dem Red Hat Satellite Server und der IP-Adresse. Deshalb erledigt die Eingabe derselben IP-Adresse für Ping-Probes auf anderen Systemen exakt dieselbe Aufgabe. Um von einem überwachten System einen

ping zu einer individuellen IP-Adresse durchzuführen, benutzen Sie stattdessen die Remote-Ping-Probe. Siehe auch Abschnitt A.8.7, „Network Services::Remote Ping“.

Tabelle A.41. Network Services::Ping Einstellungen

Feld	Wert
IP-Adress (standardmäßig System-IP)	
Pakete zu versenden*	20
Timeout*	10
Kritisch Maximale durchschnittliche Ping-Zeit	
Warnung Maximale durchschnittliche Ping-Zeit	
Kritisch Maximaler Paketverlust	
Warnung Maximaler Paketverlust	

A.8.6. Network Services::POP Mail

Die Network Services::POP Mail Probe ermittelt, ob sie zum POP3 Port auf dem System verbinden kann. Eine Portnummer muss dabei festgelegt werden: Die Abgabe einer anderen Portnummer übersteuert den Standard-Port 110. Diese Probe sammelt folgende Messdaten:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der POP-Server auf eine Verbindungs-Anforderung antwortet.

Der erforderliche **Expect (Erwarten)** Wert ist die Zeichenfolge, die nach einer erfolgreichen Verbindung zu einem POP-Server verglichen werden muss. Die Probe sucht nach der Zeichenfolge in der ersten Zeile der Rückantwort des Systems. Die Grundeinstellung ist **+OK**. Wenn der erwartete String nicht gefunden werden kann, dann meldet die Probe den Status KRITISCH zurück.

Tabelle A.42. Network Services::POP Mail Einstellungen

Feld	Wert
Port*	110
Expect*	+OK
Timeout*	10
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.7. Network Services::Remote Ping

Die Network Services::Remote Ping Probe ermittelt, ob das überwachte System mit **pingen** eine spezielle IP-Adresse erreichen kann. Der Paketverlust wird dabei ebenfalls überwacht. Die durchschnittliche Ping-Zeit (hin- und zurück) wird mit den Warnung- und Kritisch-Grenzwerten verglichen. Der erforderliche **Pakete zu senden** Wert ermöglicht es Ihnen zu kontrollieren, wieviele ICMP ECHO-Pakete zur Adresse gesendet werden. Diese Probe sammelt folgende Messdaten:

- Durchschnittliche Ping-Zeit Die Zeitspanne in Millisekunden, die ein ICMP ECHO Paket zur IP-Adresse und zurück benötigt.
- Paketverlust - Der Prozentsatz von Daten, die während dem Sendevorgang verloren gehen.

Das Feld **IP-Adresse** zeigt die genaue zu pingende Adresse an. Im Gegensatz zum ähnlichen,

optionalen Feld für die Standard-Ping-Probe, ist dies ein Pflichtfeld. Das überwachte System leitet den Ping an eine dritte Adresse um und nicht an den Red Hat Satellite Server. Da die Remote-Ping-Probe die Verbindungsfähigkeit des zu überwachenden Systems selbst überprüft, muss eine andere IP-Adresse angegeben werden. Um vom Red Hat Satellite Server aus ein System oder eine IP-Adresse zu pingen, benutzen Sie stattdessen die Standard-Ping-Probe. Siehe Abschnitt A.8.5, „Network Services::Ping“.

Anforderungen - Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem überwachten System laufen, um diesen Probe auszuführen.

Tabelle A.43. Network Services::Remote Ping Einstellungen

Feld	Wert
IP Adresse*	
Pakete zu versenden*	20
Timeout*	10
Kritisch Maximale durchschnittliche Ping-Zeit	
Warnung Maximale durchschnittliche Ping-Zeit	
Kritisch Maximaler Paketverlust	
Warnung Maximaler Paketverlust	

A.8.8. Network Services::RPCService

Die Network Services::RPCService Probe testet die Verfügbarkeit von Remote Procedure Call (RPC, ein Protokoll für verteilte Anwendungen) Programmen auf einer bestimmten IP-Adresse. Folgende Messdaten werden gesammelt:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der TCP-Server auf eine Verbindungs-Anforderung antwortet.

RPC-Serverprogramme registrieren sich selbst im RPC-Netzwerk, indem eine Programm-ID und Programmname angegeben werden. NFS ist ein Beispiel eines Dienstes, der via RPC arbeitet.

Client-Programme, welche die Ressourcen von RPC-Serverprogrammen verwenden möchten, verlangen vom Rechner (auf dem sich das Serverprogramm befindet) Zugang für RPC-Funktionen innerhalb der RPC-Programmnummer oder des Programmnamens bereitzustellen. Diese Konversationen können entweder über TCP oder UDP (beinahe immer UDP) erfolgen.

Dieser Probe lässt Sie einfach Programm-Verfügbarkeit testen. Sie müssen dabei den Progammnamen oder die Programmnummer angeben und das entsprechende Protokoll sowie die übliche Timeout-Periode.

Tabelle A.44. Network Services::RPCService Einstellungen

Feld	Wert
Protokoll (TCP/UDP)	udp
Service Name*	nfs
Timeout*	10
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.9. Network Services::Secure Web Server (HTTPS)

Die Network Services::Secure Web Server (HTTPS) Probe ermittelt Verfügbarkeit des Secure-Webservers und sammelt folgende Messdaten:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der TCP-Server auf eine Verbindungs-Anforderung antwortet.

Diese Probe meldet zurück, dass sie zum HTTPS-Port auf einem speziellen Server verbinden und die festgelegte URL aufrufen kann. Wenn keine URL festgelegt ist, wird die Probe das Root-Dokument abrufen. Die Probe hält nach einer HTTP/1.-Mitteilung vom System Ausschau, ausser Sie verändern diesen Wert. Das Festlegen einer anderen Portnummer übersteuert den Standard-Port 443.

Diese Probe unterstützt Authentifikation. Geben Sie Benutzername und Passwort in die dafür vorgesehenen Felder ein. Im Gegensatz zu den meisten anderen Probes, sendet diese Probe einen KRITISCH Status zurück, wenn diese nicht innerhalb der Timeout-Periode mit dem System in Verbindung treten kann.

Tabelle A.45. Network Services::Secure Web Server (HTTPS) Einstellungen

Feld	Wert
URL-Pfad	/
'Erwarte'-Kopfzeile	HTTP/1
'Erwarte'-Inhalt	
UserAgent*	NOCpulse-check_http/1.0
Benutzername	
Passwort	
Timeout*	10
HTTPS Port*	443
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.10. Network Services::SSH

Die Network Services::SSH Probe ermittelt die Verfügbarkeit von SSH auf dem angegebenen Port und sammelt folgende Messdaten:

- Latenz remoter Dienste - Wie lange es dauert, in Sekunden gemessen, bis der SSH-Server auf eine Verbindungs-Anforderung antwortet.

Nachdem der SSH-Server erfolgreich kontaktiert wurde und eine gültige Rückantwort erhalten wurde, zeigt die Probe die Protokoll- und Serverversions-Information an. Wenn die Probe eine ungültige Antwort erhält, zeigt diese die Mitteilung an, die sie vom Server erhalten hat und generiert einen WARNUNG Status.

Tabelle A.46. Network Services::SSH Einstellungen

Feld	Wert
SSH Port*	22
Timeout*	5
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.8.11. Network Services::Web Server (HTTP)

Die Network Services::Web Server (HTTP) Probe ermittelt die Verfügbarkeit des Webservers und sammelt folgende Messdaten:

- Remote Service Latency - Wie lange es dauert, in Sekunden gemessen, bis der HTTP-Server auf eine Verbindungs-Anforderung antwortet.

Diese Probe bestätigt, dass sie eine Verbindung mit dem HTTP Port auf dem festgelegten Server aufbauen und die festgelegte URL aufrufen kann. Wenn keine URL festgelegt ist, wird die Probe das Root-Dokument abrufen. Die Probe hält nach einer HTTP/1-Mitteilung vom System Ausschau, ausser Sie verändern diesen Wert. Die Angabe einer anderen Portnummer übersteuert den Standard-Port 80. Im Gegensatz zu den meisten anderen Probes, wird diese Probe einen KRITISCH Status zurücksenden, wenn mit dem System innerhalb der Timeout-Periode keine Verbindung zustande kommt.

Diese Probe unterstützt Authentifikation. Geben Sie Benutzername und Passwort in die entsprechenden Felder ein. Auch kann das wahlweise Virtual Host Feld verwendet werden, um ein getrenntes Dokumentations-Set zu überwachen, das sich auf derselben physischen Maschine, die als Standalone-Server dargestellt ist, befindet. Wenn Ihr Web-Server nicht konfiguriert ist virtuelle Hosts zu verwenden (was in der Regel der Fall ist), sollten Sie dieses Feld leer lassen. Wenn Sie virtuelle Hosts konfiguriert haben, geben Sie den Domain-Namen des ersten Hosts hier ein. Fügen Sie so viele Probes wie nötig hinzu, um alle virtuellen Hosts auf dem Rechner zu überwachen.

Tabelle A.47. Network Services::Web Server (HTTP) Einstellungen

Feld	Wert
URL-Pfad	/
Virtueller Host	
'Erwarte'-Kopfzeile	HTTP/1
'Erwarte'-Inhalt	
UserAgent*	NOCpulse-check_http/1.0
Benutzername	
Passwort	
Timeout*	10
HTTP Port*	80
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.9. Oracle 8i, 9i, 10g und 11g

Die Probes in diesem Abschnitt können auf den unterstützten Versionen der Oracle Datenbanken angewandt werden. Oracle Probes erfordern die Konfiguration der Datenbank und Verbindungen, indem folgender Befehl ausgeführt wird.

```
$ORACLE_HOME/rdbms/admin/catalog.sql
```

Zusätzlich dazu muss der in der Probe konfigurierte Oracle-Benutzer zumindest Privilegien, wie CONNECT und SELECT_CATALOG_ROLE besitzen, damit die Probe einwandfrei funktionieren kann.

Einige Oracle Probes sind speziell darauf ausgelegt, Einheiten für eine Langzeitsteigerung der Performance abzustimmen und nicht nur um Unterbrechungen vermeiden zu können, Aus diesem Grund empfiehlt Red Hat diese so einzuplanen, dass sie weniger häufig auftreten; zwischen einer Stunde und jeden zwei Tagen. Dies liefert eine bessere statistische Auswertung, da zumal auftretende Anomalien dadurch weniger stark hervorgehoben werden. Dies trifft auf folgende Probes zu: Buffer-Cache, Data-Dictionary-Cache, Disk-Sort-Ratio, Bibliothek-Cache und Redo-Log.

Die Grenzwerte für KRITISCH und WARNUNG dürfen nicht eine größere Zeitspanne erlauben, als diejenige, die für die Timeout-Periode gewählt wurde. Andernfalls wird ein Status UNKNOWN in allen Fällen der erweiterten Latenz zurückgegeben, wodurch die Grenzwerte beseitigt werden. Aus diesem Grund wird von Red hat dringend empfohlen, dass alle Timeout-Perioden über alle zeitbedingten Grenzwerte hinausgehen. In diesem Abschnitt bezieht sich dies speziell auf die Probe TNS-Ping.

Schlussendlich müssen Kunden, welche diese Oracle-Probes auf Oracles Multi-Threaded Server (MTS) verwenden, den Red Hat Support kontaktieren, um Einträge zur Datei /etc/hosts des Red Hat Network Servers hinzugefügt zu bekommen, um sicher zu gehen, dass der DNS-Name richtig aufgelöst wird.

A.9.1. Oracle::Active Sessions

Die Oracle::Active Sessions Probe überwacht einen Oracle-Server und sammelt folgende Messdaten:

- Aktive Sessions - Die Anzahl aktiver Sessions basierend auf dem Wert von **V$PARAMETER.PROCESSES**.
- Verfügbare Sessions - Die Prozentsatz der aktiven Sessions die verfügbar sind, die basierend auf dem Wert von **V$PARAMETER.PROCESSES**

Tabelle A.48. Oracle::Active Sessions Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Kritisch Maximale aktive Sessions	
Warnung Maximale aktive Sessions	
Kritisch Maximale verfügbare Sessions verwendet	
Warnung Maximale verfügbare Sessions verwendet	

A.9.2. Oracle::Availability

Die Oracle::Availability Probe ermittelt die Verfügbarkeit der Datenbank vom Red Hat Satellite;.

Tabelle A.49. Oracle::Availability Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30

A.9.3. Oracle::Blocking Sessions

Die Oracle::Blocking Sessions Probe überwacht einen Oracle-Server und sammelt folgende Messdaten:

- Blockierende Sessions - Die Anzahl an Sessions, welche andere Sessions davon abhalten, Änderungen in der Oracle Datenbank dauerhaft zu speichern, wie vom erforderlichen, von Ihnen zur Verfügung gestellten *Sperrzeit* Wert festgelegt. Nur die Sessions, die während der Dauer dieser Sperrrzeit blockiert haben (in Sekunden gemessen), werden als blockierende Sessions gezählt.

Tabelle A.50. Oracle::Blocking Sessions Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Sperrzeit (Sekunden)*	20
Timeout*	30
Kritisch Maximale blockierende Sessions	
Warnung Maximale blockierende Sessions	

A.9.4. Oracle::Buffer Cache

Der Oracle::Buffer Cache Probe kalkuliert die Buffer-Cache Hit Ratio, damit die SGA Datenbank Buffer-Cache-Größe optimiert werden kann. Die folgenden Messdaten werden dabei gesammelt:

- DB Block-Gets (im Cache gefundene Datenblöcke) - Die Anzahl von Blöcken, auf die via einzelner Block-Gets zugegriffen wurde (nicht durch den konsistenten Get-Mechanismus).
- Consistent Gets (im Cache gefundene Datenblöcke für die Lesekonsistenz) - Die Anzahl von Zugriffen auf den Block-Buffer, um Daten in einem konsistenten Modus wiederzuerlangen.
- Physical Reads (von Disk gelesene Datenblöcke) - Die kumulative Anzahl von Blöcken, die von Disk gelesen wurden.
- Buffer Cache Hit Ratio - Die Häufigkeit mit der die Datenbank zum Buffer anstatt zur Festplatte geht, um Daten wiederzufinden. Eine niedrige Häufigkeit legt nahe, dass das System mehr RAM benötigt.

Tabelle A.51. Oracle::Buffer Cache Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port	1521
Timeout*	30
Warnung Mimimale Buffer Cache Hit Ratio	
Kritisch Mimimale Buffer Cache Hit Ratio	

A.9.5. Oracle::Client Connectivity

Der Oracle::Client Connectivity Probe ermittelt, ob die Datenbank funktionsfähig und betriebsbereit ist und in der Lage ist, Verbindungen von den zu überwachenden Systemen zu erhalten. Dieser Probe eröffnet eine **`rhnmd`**-Verbindung zum System und führt einen **`sqlplus connect`**-Befehl auf dem überwachten System aus.

Der **`Erwarteter DB Name`**-Parameter ist der erwartete Wert von **`V$DATABASE.NAME`**. Dieser Wert unterliegt der Groß- und Kleinschreibung. Der Status KRITISCH wird zurückgemeldet, falls dieser Wert nicht gefunden werden kann.

Anforderungen — Der Red Hat Network monitoring daemon (**`rhnmd`**) muss auf dem zu überwachenden System laufen, damit diese Probe ausgeführt werden kann. Damit die Probe laufen kann muss dem **`nocpulse`** Benutzer Leseberechtigung für Ihre Protokolldateien gegeben werden.

Tabelle A.52. Oracle::Client Connectivity Einstellungen

Feld	Wert
Oracle Hostname oder IP-Adresse*	
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
ORACLE_HOME*	/opt/oracle
Erwarteter DB Name*	
Timeout*	30

A.9.6. Oracle::Data Dictionary Cache

Die Oracle::Data Dictionary Cache Probe kalkuliert die Data Dictionary Cache Hit Ratio, um die SHARED_POOL_SIZE in **`init.ora`** zu optimieren. Folgende Messdaten werden dabei gesammelt:

- Data Dictionary Hit Ratio - Die Rate von Cache-Hits im Data-Dictionary Cache. In anderen Worten beschreibt dies die Häfigkeit mit der die Datenbank auf das Dictionary zugreift, anstatt auf die Festplatte, um Daten abzurufen. Eine niedrige Häufigkeit legt nahe, dass das System mehr RAM benötigt.
- Gets - Die Anzahl von Blöcken, auf die über einzelne Block-Gets zugegriffen wurde (nicht durch den konsistenten Get-Mechanismus).

- Cache Misses - Die Anzahl von Zugriffen auf den Block-Buffer, um Daten in einem konsistenten Modus abzurufen.

Tabelle A.53. Oracle::Data Dictionary Cache Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Warnung Minmimale Data Dictionary Hit Ratio	
Kritisch Minmimale Data Dictionary Hit Ratio	

A.9.7. Oracle::Disk Sort Ratio

Die Oracle::Disk Sort Ratio Probe überwacht eine Oracle Datenbank und sammelt folgende Messdaten:

- Disk Sort Ratio - Die Häufigkeit von Oracle Sorts, die zu groß waren, um im Speicher vollständig abgeschlossen zu werden und für die stattdessen ein temporäres Segment verwendet wurde.

Tabelle A.54. Oracle::Disk Sort Ratio Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Kritisch Maximale Disk Sort Ratio	
Warnung Maximale Disk Sort Ratio	

A.9.8. Oracle::Idle Sessions

Die Oracle::Idle Sessions Probe überwacht eine Oracle-Datenbank und sammelt folgende Messdaten:

- Idle-Sessions - Die Anzahl von Oracle-Sessions, die idle (im Leerlauf) sind, wie durch den von Ihnen eingegebenen *Idle-Time*-Wert festgelegt. Nur diejenigen Sessions, die für diesen Zeitraum idle sind (in Sekunden gemessen), zählen als Idle-Sessions.

Tabelle A.55. Oracle::Idle Sessions Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Idle-Time (Sekunden)*	20
Timeout*	30
Kritisch Maximale idle Sessions	
Warnung Maximale idle Sessions	

A.9.9. Oracle::Index Extents

Die Oracle::Index Extents Probe überwacht Oracle und sammelt folgende Messdaten:

- Zugeordnete Bereiche - Die Anzahl an zugeordneten Bereiche für jeden Index.
- Verfügbare Bereiche - Der Prozentsatz an zugeordneten Bereichen für jeden Index.

Das Mussfeld **`Index Name`** beinhaltet den Standardwert **%**, der mit jedem Index Namen übereinstimmt.

Tabelle A.56. Oracle::Index Bereichs Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Index Eigentümer*	%
Index Name*	%
Timeout*	30
Kritisch Maximum an zugeordneten Bereichen	
Warnung Maximum an zugeordneten Bereichen	
Kritisch Maximum an zugeordneten Bereichen	
Warnung Maximum an zugeordneten Bereichen	

A.9.10. Oracle::Library Cache

Die Oracle::Library Cache Probe kalkuliert die Library Cache Miss Ratio, um SHARED_POOL_SIZE in **`init.ora`** zu optimieren. Folgende Messdaten werden gesammelt:

- Library Cache Miss Ratio - Die Häufigkeit in der ein Library Cache Pin Miss auftritt. Dies passiert, wenn eine Session ein Statement ausführt, das bereits analysiert wurde, sich aber nicht mehr länger im gemeinsam benutzten Pool befindet.
- Ausführungen - Wie oft um einen Pin für Objekte in diesem Namensraum angefragt worden ist.
- Cache Misses - Die Anzahl von Pins, die jetzt das Objekt von der Disk abrufen müssen. Diese Pins werden aus Objekten mit früheren Pins, ab dem Zeitpunkt der Objekt-Handle Erstellung, hergestellt.

Tabelle A.57. Oracle::Library Cache Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Kritisch Maximale Library Cache Miss Ratio	
Warnung Maximale Library Cache Miss Ratio	

A.9.11. Oracle::Locks

Die Oracle::Locks Probe überwacht eine Oracle Datenbank und sammelt folgende Messdaten:

- Aktive Locks - Die aktuelle Anzahl an aktiven Locks, wie vom Wert in der v$locks-Tabelle festgelegt. Datenbank-Admininstratoren sollten sich einer hohen Anzahl an Locks in einer Datenbank-Instanz bewusst sein.

Locks werden verwendet damit mehrere Benutzer und Prozesse, welche dieselben Daten in der Datenbank aktualisieren, nicht kollidieren. Diese Probe ist nützlich die Datenbank-Administratoren zu warnen, wenn einen hohe Anzahl von Locks in einer bestimmten Instanz vorhanden sind.

Tabelle A.58. Oracle::Locks Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Kritisch Maximale Aktive Locks	
Warnung Maximale Aktive Locks	

A.9.12. Oracle::Redo Log

Die Oracle::Redo Log Probe überwacht eine Oracle-Datenbank und sammelt folgende Messdaten:

- Redo Log Space Anfragerate - Die durchschnittliche Anzahl von Redo Log Space Anfragen pro Minute seit dem Starten des Servers.
- Redo Buffer Allocation Retry Rate (Zuordnungs-Wiederholungsrate) - Die durchschnittliche Anzahl von Bufferzuordnungs-Wiederholungen pro Minute seit dem Starten des Servers.

Die erhaltenen Messdaten und die Grenzwerte, mit denen diese verglichen werden, sind Zahlen, welche die Änderungsrate von Ereignissen pro Minute darstellen. Diese Änderungsrate sollte überwacht werden, da schnelles Wachstum Probleme hervorrufen kann, die untersucht werden müssen.

Tabelle A.59. Oracle::Redo Log Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Kritisch Maximale Redo Log Space Anfragerate	
Warnung Maximale Redo Log Space Anfragerate	
Kritisch Maximale Wiederholungsrate der Redo Bufferzuweisung	
Warnung Maximale Wiederholungsrate der Redo Bufferzuweisung	

A.9.13. Oracle::Table Extents

Die Oracle::Table Extents Probe überwacht eine Oracle Datenbank und sammelt folgende Messwerte:

- Zugewiesen Erweiterungen (beliebige Tabelle) - Die Gesamtanzahl an Erweiterungen für eine beliebige Tabelle.
- Verfügbare Erweiterungen (beliebige Tabelle) - Der Prozentsatz von verfügbaren Erweiterungen für eine beliebige Tabelle.

In Oracle ermöglichen Tabellen-Erweiterungen das Wachstum einer Tabelle. Wenn eine Tabelle voll ist, wird diese um eine bestimmte Menge an Platz *erweitert*, welche bei der Erstellung der Tabelle festgelegt wurde. Erweiterungen werden auf einer Pro-Tabelle-Basis mit einer Erweiterungsgröße und einer maximalen Anzahl von Erweiterungen konfiguriert.

Eine Tabelle, die beispielsweise ursprünglich 10 MB aufweist und mit einer Erweiterungsgröße von 1 MB konfiguriert ist und maximal 10 Erweiterungen erhalten kann, kann bis zu maximal 20 MB anwachsen. Diese Probe kann entweder nach (1) Anzahl der zugewiesenen Extends warnen (z.B. Status wird kritisch, wenn 5 mal oder öfter erweitert worden ist) oder (2) die Tabelle einen bestimmten Prozentsatz der maximaler Erweiterungen überschritten hat (z.B. Status wird kritisch, wenn 80% oder mehr der möglichen Erweiterungen bereits stattgefunden haben).

Die Mussfelder **`Tabellen-Besitzer`** und **`Tabellenname`** beinhalten den Standardwert `%`, welcher jedem Tabellen-Besitzer oder -Namen entspricht.

Tabelle A.60. Oracle::Table Extents Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Tabellen-Besitzer*	%
Tabellen-Name*	%
Timeout*	30
Kritisch Maximale zugewiesene Extends	
Warnung Maximale zugewiesene Extends	
Kritisch Maximale verfügbare Extends	
Warnung Maximale Verfügbare Extends	

A.9.14. Oracle::Tablespace Usage

Die Oracle::Tablespace Usage Probe überwacht eine Oracle Datenbank und sammelt folgende Messwerte:

- Verfügbarer Speicherplatz Verwendet - Der Prozentsatz von verfügbarem Speicher, der in jedem Tabellenbereich verwendet wurde.

Tabellenbereich ist der gemeinsame Pool von Speicherplatz, in die Tabellen, Indizes und andere Datenobjekte geschrieben werden. Diese Probe gibt eine Warnung aus, wenn der gesamte verfügbare Speicherplatz unter dem Grenzwert liegt. Tabellenbereich wird in Bytes gemessen, sodass Erweiterungen keine direkte Rolle spielen (obwohl jede Erweiterung verfügbaren Platz vom gemeinsamen Pool entfernt).

Das Mussfeld **`Tabellenbereich Name`** unterliegt der Groß- und Kleinschreibung und beinhaltet einen Standardwert `%`, welcher mit jedem beliebigem Tabellennamen übereinstimmt.

Tabelle A.61. Oracle::Tablespace Usage Einstellungen

Feld	Wert
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Tabellenbereich Name*	%
Timeout*	30
Kritisch Maximaler Verbrauch verfügbaren Speicherplatzes	
Warnung Maximaler Verbrauch verfügbaren Speicherplatzes	

A.9.15. Oracle::TNS Ping

Die Oracle::TNS Ping Probe ermittelt ob ein Oracle-Listener auf Anfragen vom Netzwerk antwortet und sammelt folgende Messdaten:

- Latenz Externer Dienste - Wie lange es dauert, in Sekunden gemessen, bis der Oracle-Server auf eine Verbindungsanfrage antwortet.

Tabelle A.62. Oracle::TNS Ping Einstellungen

Feld	Wert
TNS Listener Port*	1521
Timeout*	15
Kritisch Maximale Externer Dienst Latenz	
Warnung Maximale Externer Dienst Latenz	

A.10. Red Hat Satellite

Die Probes in diesem Abschnitt können für den Red Hat Satellite selbst angewandt werden, um dessen Betriebsfähigkeit und Performance zu überprüfen. Da diese Probes lokal laufen, sind keine speziellen Applikationen oder Transportprotokolle notwendig.

A.10.1. Red Hat Satellite::Disk Space

Die Red Hat Satellite::Disk Space Probe ermittelt den freien Plattenplatz auf einem Satellite und sammelt folgende Messdaten:

- Verwendetes Dateisystem - Der Prozentsatz des aktuellen Dateisystems, das sich derzeit in Verwendung befindet.
- Verwendeter Speicherplatz - Die Dateigröße, die vom aktuellen Dateisystem verwendet wird.
- Verfügbarer Speicherplatz - Die Dateigröße, die dem aktuellen Dateisystem zu Verfügung steht.

Tabelle A.63. Red Hat Satellite::Disk Space Einstellungen

Feld	Wert
Einheit Pfadname*	/dev/hda1
Kritisch Maximal verwendetes Dateisystem	
Warnung Maximal verwendetes Dateisystem	
Critical Maximum Space Used (Kritisch - Maximal verwendeter Platz)	
Warning Maximum Space Used (Warnung - Maximal verwendeter Platz)	
Kritisch Maximaler verfügbarer Speicherplatz	
Warnung Maximaler verfügbarer Speicherplatz	

A.10.2. Red Hat Satellite::Ausführungszeit

Die Red Hat Satellite::Ausführungszeit Probe ermittelt die Ausführungszeit für Probes, die vom Satellite ausgeführt werden und sammelt folgende Messdaten:

- Durchschnittliche Proben-Ausführungszeit - Die Sekunden, die eine Probe benötigt, um vollständig ausgeführt zu werden.

Tabelle A.64. Red Hat Satellite::Ausführungszeit Einstellungen

Feld	Wert
Kritisch Maximale Durchschnittliche Probe-Ausführungszeit	
Warnung Maximale Durchschnittliche Probe-Ausführungszeit	

A.10.3. Red Hat Satellite::Schnittstellen Verkehr

Die Red hat Satellite::Schnittstellen Verkehr Probe ermittelt den Schnittstellenverkehr auf einem Satellite und sammelt folgende Messdaten:

- Eingangsrate - Die in Bytes pro Sekunde gemessene Menge an Verkehr, welchen die Einheit erhält.
- Ausgangsrate - Die in Bytes pro Sekunde gemessene Menge an Verkehr, welcher von der Einheit gesendet wird.

Tabelle A.65. Red Hat Satellite::Schnittstellen Verkehr Einstellungen

Feld	Wert
Interface * (Schnittstelle*)	eth0
Timeout (Sekunden)*	30
Critical Maximum Input Rate (Kritisch - Maximale Eingangsrate)	
Critical Maximum Output Rate (Kritisch - Maximale Ausgangsrate)	

A.10.4. Red Hat Satellite::Latenz

Die Red Hat Satellite::Latenz Probe überwacht die Latenz von Probes auf einem Satellite und sammelt folgende Messdaten:

- Durchschnittliche Probe-Latenz - Die zeitliche Verzögerung in Sekunden ab dem Zeitpunkt, an dem eine Probe startbereit ist und bis zum Zeitpunkt, an dem die Probe tatsächlich abläuft. Unter normalen Umständen ist dies für gewöhnlich weniger als eine Sekunde. Wenn ein Satellite überladen ist (weil zu viele Probes in Bezug auf ihre durchschnittlichen Ausführungszeit vorhanden sind), erhöht dies die Messzahl.

Tabelle A.66. Red Hat Satellite::Latenz Einstellungen

Feld	Wert
Kritisch Maximaler Probe-Latenzdurchschnitt	
Warnung Maximaler Probe-Latenzdurchschnitt	

A.10.5. Red Hat Satellite::Auslastung

Die Red Hat Satellite::Auslastung Probe ermittelt die CPU-Auslastung auf einem Satellite and sammelt die folgenden Messdaten:

- Auslastung - Der Auslastungsdurchschnitt auf der CPU für eine 1-, 5- und 15-minütige Periode.

Tabelle A.67. Red Hat Satellite::Auslastung Einstellungen

Feld	Wert
Kritisch Maximaler 1-minütiger Durchschnitt	
Warnung Maximaler 1-minütiger Durchschnitt	
Kritisch Maximaler 5-minütiger Durchschnitt	
Warnung Maximaler 5-minütiger Durchschnitt	
Kritisch Maximaler 15-minütiger Durchschnitt	
Warnung Maximaler 15-minütiger Durchschnitt	

A.10.6. Red Hat Satellite::Probe Anzahl

Die Red Hat Satellite::Probe Anzahl Probe ermittelt die Anzahl von Probes auf einem Satellite und sammelt folgende Messdaten:

- Probes - Die Anzahl von individuellen Probes, die auf einem Satellite laufen.

Tabelle A.68. Red Hat Satellite::Probe Anzahl Einstellungen

Feld	Wert
Kritisch Maximale Probe-Anzahl	
Warnung Maximale Probe-Anzahl	

A.10.7. Red Hat Satellite::Prozess-Anzahl

Die Red Hat Satellite::Prozess-Anzahl Probe ermittelt die Anzahl von Prozessen auf einem Satellite und sammelt folgende Messdaten:

- Blockiert - Die Anzahl von Prozessen, die in die Warteschlange und in den Warte-Status gewechselt wurden.
- Child (Kind) - Die Anzahl von Prozessen, die von einem anderen Prozess erzeugt werden, der bereits auf dem Rechner läuft.
- Defunct (Nicht mehr bestehend)- Die Anzahl an abgebrochenen Prozessen (entweder von einem Signal gelöscht oder durch Aufruf von **`exit()`**), dessen Elternprozesse noch keine Benachrichtigung erhalten haben, indem (eine Form von) **`wait()`** Systemaufruf ausgeführt wurde.
- Stopped (Angehalten) - Die Anzahl von Prozessen, die vor der vollständigen Ausführung angehalten wurden.
- Sleeping (Ruhezustand) - Ein Prozess, der sich im **`Interruptible`** (unterbrechbaren) Ruhezustand befindet, der später wieder in den Speicher eingeführt werden kann und die Ausführung dort wieder aufnimmt, wo er aufgehört hat.

Tabelle A.69. Red Hat Satellite::Prozess-Anzahl Einstellungen

Feld	Wert
Critical Maximum Blocked Processes (Kritisch - Maximal gesperrte Prozesse)	
Warning Maximum Blocked Processes (Warnung - Maximal gesperrte Prozesse)	
Critical Maximum Child Processes (Kritisch - Maximale Kindprozesse)	
Warning Maximum Child Processes (Warnung - Maximale Kindprozesse)	
Critical Maximum Defunct Processes (Kritisch - Maximal nicht mehr bestehende Prozesse)	
Warning Maximum Defunct Processes (Warnung - Maximal nicht mehr bestehende Prozesse)	
Critical Maximum Stopped Processes (Kritisch - Maximal angehaltene Prozesse)	
Warning Maximum Stopped Processes (Warnung - Maximale Angehaltene Prozesse)	
Critical Maximum Sleeping Processes (Kritisch - Maximal schlafende Prozesse)	
Warning Maximum Sleeping Processes (Warnung - Maximal schlafende Prozesse)	

A.10.8. Red Hat Satellite::Prozesse

Die Red Hat Satellite::Prozesse Probe überwacht die Anzahl von Prozessen auf einem Satellite und sammelt folgende Messdaten:

- Prozesse - Die Anzahl an Prozessen, die gleichzeitig auf der Maschine laufen.

Tabelle A.70. Red Hat Satellite::Prozesse Einstellungen

Feld	Wert
Kritisch Maximale Prozesse	
Warnung Maximale Prozesse	

A.10.9. Red Hat Satellite::Prozess Gesundheit

Die Red Hat Satellite::Prozess Gesundheit Probe überwacht kunden-spezifische Prozesse und sammelt folgende Messdaten:

- CPU-Verbrauch - Der in Prozent gemessene CPU-Verbrauch eines bestimmten Prozesses.
- Child Process Groups - Die Anzahl von Kindprozessen, die vom spezifizierten Elternprozess erzeugt werden. Ein Kindprozess übernimmt die meisten Attribute, wie beispielsweise offene Dateien, vom seinem Elternprozess.
- Threads - Die Anzahl laufender Threads für einen bestimmten Prozess. Ein Thread ist ein Ausführungsstrang innerhalb eines Prozesses (Grundeinheit der CPU-Auslastung) und besteht aus einem sogenannten Befehlszähler, einem Register-Satz und einem Stacksegment. Ein Thread wird

auch als 'Leichtgewichtprozess' bezeichnet.

- Verbrauch an physischem Speicher -Die Menge an physischem Speicher in Kilobytes, der vom festgelegten Prozess verwendet wird.
- Virtual Memory Used (Verbrauchter virtueller Speicher) - Die Menge an virtuellem Speicher in Kilobytes, die vom angegebenen Prozess verwendet wird oder die Größe des Prozesses im Realspeicher plus Swap.

Legen Sie den Prozess entweder anhand dem Befehlsnamen oder der Prozess ID (PID) fest. Wenn Sie eine PID eingeben, dann übersteuert diese den Befehlsnamen. Wenn weder Befehlsname noch PID eingetragen sind, wird der Fehler Command not found (Befehl nicht gefunden) angezeigt und die Probe auf den KRITISCH Status gesetzt.

Tabelle A.71. Red Hat Satellite::Prozess Gesundheit Einstellungen

Feld	Wert
Command Name (Befehlsname)	
Process ID (PID) file (Prozess ID (PID) Datei)	
Timeout*	15
Critical Maximum CPU Usage (Kritisch - Maximaler CPU-Verbrauch)	
Warning Maximum CPU Usage (Warnung - Maximaler CPU-Verbrauch)	
Critical Maximum Child Process Groups (Kritisch - Maximale Kindprozess-Gruppen)	
Warning Maximum Child Process Groups (Warnung - Maximale Kindprozess-Gruppen)	
Critical Maximum Threads (Kritisch - Maximale Threads)	
Warning Maximum Threads (Warnung - Maximale Threads)	
Critical Maximum Physical Memory Used (Kritisch - Maximal verbrauchter physischer Speicher)	
Warning Maximum Physical Memory Used (Warnung - Maximal verbrauchter physischer Speicher)	
Critical Maximum Virtual Memory Used (Kritisch - Maximaler verbrauchter virtueller Speicher)	
Warning Maximum Virtual Memory Used (Warnung - Maximaler verbrauchter virtueller Speicher)	

A.10.10. Red Hat Satellite::Prozess Laufend

Die Red Hat Satellite::Prozess Laufend Probe stellt sicher, dass der angegebene Prozess läuft. Legen Sie den Prozess mittels Befehlsname oder PID fest. Die Eingabe einer Prozess-ID übersteuert den Eintrag eines Befehlsnamens. Ein Kritischer Status resultiert, wenn die Probe den Befehl oder die PID nicht verifizieren kann.

Tabelle A.72. Red Hat Satellite::Prozess Laufend Einstellungen

Feld	Wert
Command Name (Befehlsname)	
Process ID (PID) file (Prozess ID (PID) Datei)	
Kritisch Maximale Anzahl laufender Prozesse	
Kritisch Maximale Anzahl ablaufender Prozesse	

A.10.11. Red Hat Satellite::Swap

Die Red Hat Satellite::Swap Probe überwacht den Prozentsatz an freiem Swap-Space, der auf einem Satellite verfügbar ist. Wenn der gemessenen Wert unter dem kritischen Grenzwert liegt, dann liegt der Status KRITISCH vor. Der Status WARNUNG wird ausgegeben, wenn der Wert unter dem Warnung-Grenzwert liegt.

Tabelle A.73. Red Hat Satellite::Swap Einstellungen

Feld	Wert
Kritisch Maximaler freier Swap-Prozentsatz	
Warnung Maximaler freier Swap-Prozentsatz	

A.10.12. Red Hat Satellite::Users

Die Red Hat Satellite::Users Probe überwacht die Anzahl von Benutzern, die aktuell im Satellite angemeldet sind. Ein KRITISCH Status besagt, dass der Wert über den dafür angelegten Grenzwert hinausgeht. Bei einem WARNUNG-Status übersteigt der Wert den Warnung-Grenzwert.

Tabelle A.74. Red Hat Satellite::Users Einstellungen

Feld	Wert
Kritisch Maximale Benutzeranzahl	
Warnung Maximale Benutzeranzahl	

Versionsgeschichte

Version 4-32.1.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Version 4-32.1 **Fri Aug 30 2013** **Rainer Gromansperg**
Brewed for de-DE

Version 4-32.1 **Fri Aug 30 2013** **Terry Chuang**
Übersetzungsdateien synchronisiert mit XML-Quellen 4-32

Version 4-32 **Thu Aug 29 2013** **Dan Macpherson**
Erste Umsetzung der Rückinformation von der QE-Prüfung

Version 4-31 **Tue Aug 27 2013** **Dan Macpherson**
Kleine Änderungen

Version 4-30 **Tue Aug 27 2013** **Dan Macpherson**
Finale QE-Implementierung

Version 4-29 **Tue Aug 27 2013** **Dan Macpherson**
Bildschirm-Texte berichtigen

Version 4-28 **Tue Aug 27 2013** **Dan Macpherson**
Entfernen von computeroutput-Tags

Version 4-27 **Tue Aug 27 2013** **Dan Macpherson**
Feedback von BZ#1001385 implementiert

Version 4-26 **Tue Aug 27 2013** **Dan Macpherson**
QE-Feedback von BZ#1001385 implementiert

Version 4-25 **Tue Aug 27 2013** **Dan Macpherson**
Tippfehler behoben für BZ#1001378

Version 4-24 **Tue Aug 27 2013** **Dan Macpherson**
QE-Feedback basierend auf BZ#1001378 und BZ#1001379 implementiert

Version 4-23 **Tue Aug 27 2013** **Dan Macpherson**
QE-Feedback von BZ#1001376 implementiert

Version 4-22 **Thu Aug 15 2013** **Dan Macpherson**
Tippfehler Korrekturen von QE Durchsicht

Version 4-21 **Sun Jul 28 2013** **Dan Macpherson**
Zweite Umsetzung der Rückinformation von der Technischen Revision

Version 4-20 **Wed Jul 24 2013** **Dan Macpherson**
Korrekturen für BZ#987245

Version 4-19 **Tue Jul 23 2013** **Dan Macpherson**

Erste Umsetzung der Rückinformation von der Technischen Revision

Version 4-18 **Thu Jul 12 2013** **Dan Macpherson**

Endgültige Beta Updates

Version 4-17 **Thu Jul 12 2013** **Dan Macpherson**

Beta Update

Version 4-16 **Thu Jul 11 2013** **Athene Chan**

Splice Abschnitt bearbeitet.
Weiteren ISS Inhalt hinzugefügt.

Version 4-15 **Fri Jul 5 2013** **Athene Chan**

BZ#906577 ISS bearbeitet nach Entwickler-Revision.

Version 4-14 **Fri Jul 5 2013** **Athene Chan**

BZ#906577 Zusätzliche Information über neue Funktionen von ISS hinzugefügt.

Version 4-13 **Fri June 28 2013** **Athene Chan**

Alle Abschnitte aktualisiert auf Basis der aktualisierten UI Änderungen.
Änderung von "Red Hat Proxy" auf "Red Hat Satellite Proxy" auf Basis der Marken-Namensänderung.
BZ#906577 Zusätzliche Information über Intersatellite-sync zum Handbuch hinzugefügt.

Version 4-12 **Tue June 4 2013** **Athene Chan**

BZ#969091 Veränderte veralteten Dateinamen von /etc/rhn/rhn_web.conf auf /etc/rhn/rhn.conf.

Version 4-11 **Fri May 17 2013** **Athene Chan**

Handbuch-Prozeduren auf Basis des Benutzer-Interface bearbeitet.
Handbuch zwecks Revision erzeugt.

Version 4-10 **Thu Apr 25 2013** **Athene Chan**

BZ#908911 Alle Referenzen auf up2date wurden auf die aktuellen Versionen geändert.
BZ#927113, 950295 Handbuch Abstrakt wurde aktualisiert
BZ#927546, 924221 Geringe Änderungen an Standardisierten Begriffen
Inhalt für die nächste Versions-Release bearbeitet.

Version 4-9 **Thu Feb 28 2013** **Athene Chan**

Inhalts-Verzeichnis in Vorbereitung für die nächste Versions-Release bearbeitet.

Version 4-8 **Wed Jan 2 2013** **Athene Chan**

BZ#862950 Leerzeichen zwischen "(pup)" und "that" in en_US-Sprachversion eingefügt.

Version 4-7 **Wed Sept 19 2012** **Dan Macpherson**

Finale Zusammenstellung für 5.5

Version 4-6 **Thu Aug 16 2012** **Athene Chan**

BZ#847993 Dateiname in Beispiel geändert in Abschnitt 5.2.4

Version 4-5	**Thu Aug 16 2012**	**Athene Chan**

BZ#773647 Absätze mit Bezug auf den Screenshot "Neuen Account erstellen" aktualisiert
BZ#846691 "Kaufen" Link in Abschnitt 1.1 aktualisiert

Version 4-4	**Wed Aug 15 2012**	**Athene Chan**

BZ#773647 Screenshot "Neuen Account erstellen" aktualisiert

Version 4-3	**Thu Aug 9 2012**	**Athene Chan**

Staging des Dokuments zwecks Revision

Version 3-2	**Fri Aug 3 2012**	**Athene Chan**

BZ#844849 Absatz umstrukturiert.

Version 3-1	**Tue Jun 17 2012**	**Athene Chan**

Veraltete Inhalte entfernt. Vorbereitet für 5.5 Release
BZ#837703 Hinweis für benutzerdefinierte GPG-Schlüssel hinzugefügt

Version 3-0	**Thurs May 24 2012**	**Athene Chan**

BZ#783340 - "s390x" auf "IBM System z" aktualisiert

Version 2-6	**Mon Jan 9 2012**	**Lana Brindley**

BZ#707591 - Virtualisierungskapitel - Anweisungen aktualisiert
BZ#746640 - Virtualisierungskapitel - Kickstart-Informationen hinzugefügt

Version 2-5	**Wed Jan 4 2012**	**Lana Brindley**

BZ#707568 & BZ#707570 - Virtualisierungskapitel - Channel-Namen
BZ#744653 - Virtualisierungskapitel - Tippfehler
BZ#744656 - Virtualisierungskapitel - RHEL6-Anweisungen aktualisiert
BZ#750481 - Methode zur Änderung der maximalen Dateigröße aktualisiert
BZ#766424 - Kickstart-Kapitel - Text aktualisiert

Version 2-4	**Fri Sep 23 2011**	**Lana Brindley**

BZ#702516 - Unix-Handbuch
BZ#703605 - Monitoring-Kapitel
BZ#706868 & BZ#707169 - Cobbler-Kapitel
BZ#707591 - Virtualisierungskapitel
BZ#707602 - Virtualisierungskapitel
BZ#715267 - Tippfehler

Version 2-3	**Mon Aug 15 2011**	**Lana Brindley**

Änderungen der z-Stream Release in y-Stream-Release eingebracht

Version 2-2	**Wed Jun 15 2011**	**Lana Brindley**

Vorbereitet für Übersetzung

Version 2-1	**Fri May 27 2011**	**Lana Brindley**

Änderungen von Übersetzern

Version 2-0	**Fri May 6 2011**	**Lana Brindley**

Vorbereitet für Übersetzung

Version 1-29 **Fri March 25 2011** **Lana Brindley**

Entitys für Übersetzung korrigiert
BZ#683466 - Monitoring

Version 1-28 **Thu March 24 2011** **Lana Brindley**

BZ#679621 - Entities für Übersetzung korrigiert
BZ#681788 - Benachrichtigungen

Version 1-27 **Mon Feb 14 2011** **Lana Brindley**

BZ#658127 - API-Zugriff

Version 1-26 **Wed Feb 9 2011** **Lana Brindley**

BZ#658120 - Hinweise auf RHEL 2.1 entfernt
BZ#658131 - API-Zugriff
BZ#669166 - Virtualisierung

Version 1-25 **Mon Jan 31 2011** **Lana Brindley**

BZ#443630 - Kickstart
BZ#559515 - Cobbler